УДК 004.942: 004.49: 004.056.57

А.С. Бычков, В. Новотна, В.Л. Шевченко, А.В. Шевченко

СОВЕРШЕНСТВОВАНИЕ МОДЕЛИ КОМПЬЮТЕРНЫХ ЭПИДЕМИЙ НА ОСНОВЕ РАСШИРЕНИЯ МНОЖЕСТВА ВОЗМОЖНЫХ СОСТОЯНИЙ ОБЪЕКТОВ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Ключевые слова: компьютерные эпидемии, модель, управление, состояние объекта.

Введение

Компьютерные атаки на информационные системы (ИС) государственных учреждений, объектов критической инфраструктуры, банковского сектора, бизнеса приобрели глобальный эпидемиологический характер [1]. Для эффективного противодействия атакам необходимо прогнозировать их развитие. Актуальным является усовершенствование моделей компьютерных эпидемий и определение управляющих параметров, обеспечивающих сдерживание эпидемий в безопасных пределах. Изначально современные модели компьютерных эпидемий строились на основе моделей биологических эпидемий. Для повышения качества моделей нужно обобщить существующий опыт, найти слабые места, усовершенствовать модели и проверить их на примере известных эпидемий.

Цель статьи — усовершенствование существующих моделей компьютерных эпидемий на основе выявления неучтенных состояний объектов информационных систем.

Подобие биологических и компьютерных эпидемий выявлено достаточно давно [2, 3]. Общим недостатком первых моделей — SI, SIS, SIR — является чрезмерное упрощение. С начала 2000-х годов трансформация опыта моделирования биологических эпидемий в компьютерную отрасль стала более целенаправленной и системной [4]. Новый толчок к развитию дало появление червя Code Red: 13.06.2001 версия CRv1 [5] и 19.07.2001 версия CRv2 [6, 7]. Созданная по результатам эпидемии Code Red модель RCS (Random Constant Spread) дала хорошее совпадение прогнозных и статистических данных по эпидемиям червей CRv1, CRv2, SQL Slammer [5, 8]. Однако при эпидемии SQL Slammer RCS прогноз совпал со статистикой только в первой части заражения. Далее модель показывала рост эпидемии, однако сеть оказалась неспособной обслуживать такое большое количество запросов от SQL Slammer. Это лишний раз подтверждает мысль о том, что высокая скорость сети нужна там, где она действительно необходима. Для профилактики информационной безопасности можно снижать быстродействие. На рост эпидемии также влияет топология сети [9–12]. Однако ускорение роста компьютерных эпидемий привело к тому, что большинство топологий ведут себя подобно модели «каждый с каждым», которая и принята в качестве базовой в данном исследовании.

1. Возможные состояния атакованных объектов ИС и их обозначения

P_0 (Population) [13] — суммарное количество объектов в системе (популяция — в случае биологической эпидемии). В [14] обозначено как N (Number); N_0 (Not

susceptible) — невосприимчивые к заражению еще до начала эпидемии из-за отсутствия объекта в зоне заражения или вследствие высокого уровня защиты (обозначение введено авторами). В [8] — *M* (passive iMmunity); *S* (Susceptible) [9] — здоровые и восприимчивые к заражению; *E* (Exposed) [9] — доступные, незащищенные (в биологическом мире — инкубационный период). В компьютерных системах состояние, в котором вредоносное программное обеспечение уже проникло в ИС, пока не вредит, но готовится дать доступ к системе основному вредоносному коду. В [15] отмечено как *L* (latent); *n* [16] — количество стадий инкубационного периода; *B* (Breaking-out) [15] — проявления заражения. В [17] обозначено как *A* (Active); *D* (Detected) [9] — вредоносный код выявлен, но противодействие еще не началось; *I* (Infected) [9] — объект заражен и активно заражает другие объекты; *m* — количество стадий заражения. В [16] предусмотрено *n* стадий инкубационного периода и *m* стадий инфекционного заболевания; *Q* (Quarantine) [15] — объекты, переведенные в карантин; *P* (Patched) [18] — состояние установки заплаток для устранения выявленных уязвимостей. При этом массовые полезные действия по устранению уязвимостей перегружают сеть и могут приводить к «отказу в обслуживании» (DoS, Denial of Service); N_1 (Not susceptible) или *R* (Removed, Recovered) — вылечен и получил иммунитет. Зачастую обозначается как *R* [9], но если есть опасность смешения понятий, то лучше применить *N*1. Реже используют обозначения *A* (Antidot, Antivirus) [14], *M* (iMmune — получил иммунитет) [4, 18]; *F* (Fatal) [17] — безвозвратно утраченные (погибшие) объекты. Для ИС — узлы, которые не подлежат восстановлению в течение жизненного цикла ИС.

Компоненты вектора состояния ИС обозначим $Y = \{N, S, E, I, B, D, R, Q, W, F...\}$ мнемонически или цифровыми индексами $Y = \{y_1, y_2, ..., y_r\}$. Переходы между состояниями описывают уравнения Колмогорова в виде обыкновенных дифференциальных уравнений. Для графического представления моделей используем цепи Маркова, которые определяют возможные переходы между состояниями (рис. 1). Круг с пометкой соответствует конкретному состоянию. Стрелки обозначают направления возможных переходов.

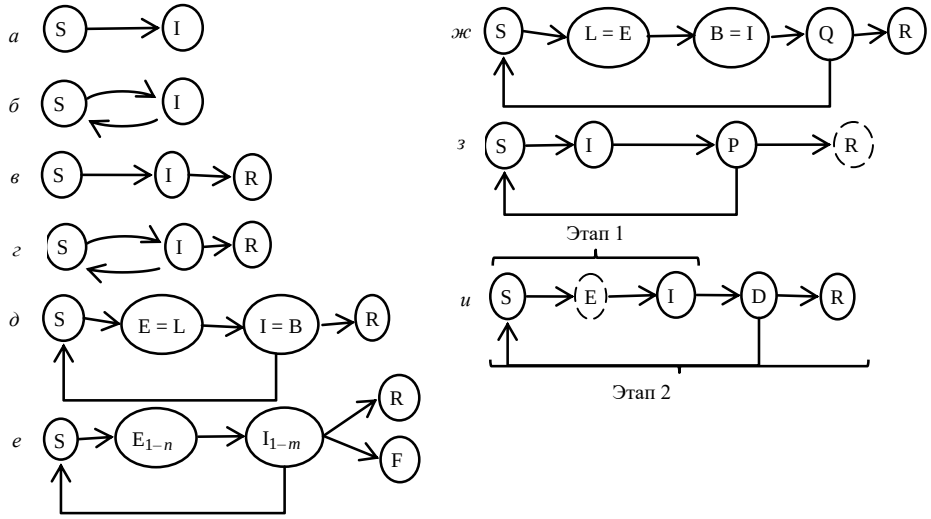


Рис. 1

2. Эволюция моделей компьютерных эпидемий

Уточним следующие обозначения: E, E_i — количество объектов, инфицированных на разных стадиях, $i = \overline{1, n}$, латентного периода (без индексов — суммар-

ное количество); I, I_j — количество объектов, инфицированных на разных стадиях, $j=\overline{1,m}$, активного периода (без индексов — суммарное количество); τ_{E_i} — длительность разных стадий, $i=\overline{1,n}$, латентного периода заражения; τ_{I_j} — длительность разных стадий, $j=\overline{1,m}$, активного периода заражения; K_{SI}, K_{IS}, K_{IR}, K_{IF} — коэффициенты интенсивности переходов между различными состояниями. Первый индекс показывает начальное состояние, второй — конечное.

С учетом принятых обозначений рассмотрим известные виды моделей эпидемий.

SI — объект может быть восприимчив к заражению *S* либо болен *I* (рис. 1, *а*). Лечение и выздоровление не предусмотрены. В зависимости от верхнего ограничения на количество больных, модель делится на два подвида; SI exp — экспоненциальное развитие. Количество больных может расти бесконечно. Уравнения динамики развития:

$$\frac{dI}{dt} = K_{SI} I.$$

SI SL — *S*-образное (логистическое) развитие. Количество зараженных объектов ограничено суммарным количеством всех объектов (размер популяции, количество компьютеров в сети с учетом ее пропускной способности, как это было с червем SQL Slammer). Уравнения динамики развития:

$$\frac{dI}{dt} = K_{SI} I(P_0 - I).$$

SIS — объект может избавиться от заражения, но иммунитета при этом не приобретает и вновь переходит в состояние *S* (рис. 1, *б*). Уравнения динамики развития:

$$\frac{dI}{dt} = K_{SI} I(P_0 - I) - K_{IS} I;$$

$$S = P_0 - I.$$

SIR [19] — объект не только избавляется от заражения, но и получает иммунитет *R* [20, 21] (рис. 1, *в*). SIR(*t*) [9] — все так же, как в модели SIR, но коэффициенты перехода из состояния *S* в *R* изменяются во времени. Модель SIR — частный случай модели SIR(*t*).

$$\frac{dI}{dt} = K_{SI}(t) I(P_0 - I) - K_{IR}(t) I;$$

$$\frac{dR}{dt} = K_{IR}(t) I;$$

$$S = P_0 - I - R.$$

SIRI [22] — объект избавляется от заражения, но иммунитет получает только часть объектов *R*, а другая часть *S* может быть вновь зараженной (рис. 1, *г*).

$$\frac{dI}{dt} = K_{SI} I(P_0 - I) - K_{IR} I - K_{IS} I;$$

$$\frac{dR}{dt} = K_{IR} I;$$

$$\frac{dS}{dt} = K_{IS} I.$$

SEIR — добавляется латентный (скрытый) период τ_E развития инфицирования E, когда заражение уже произошло, но активных действий инфекция пока не предпринимает (рис. 1, *д*). В [10, 18] аналогичную модель называют SLBS.

$$\frac{dE}{dt} = K_{SI} I(P_0 - I) - K_{IR} I - K_{IS} I;$$

$$I = E(t - \tau_E);$$

$$\frac{dR}{dt} = K_{IR} I;$$

$$\frac{dS}{dt} = K_{IS} I.$$

SEnImRF [17] — в модели SEIR дополнительно учтено количество стадий инкубационного периода n и количество стадий активного заражения m. Продолжительность соответствующих стадий равна τ_{E_i}, $i = \overline{1, n}$; τ_{I_j}, $j = \overline{1, m}$. Также введено состояние F полностью утраченных (погибших) объектов (рис. 1, *е*).

$$I = \sum_{i=1}^{m} I_i;$$

$$\frac{dE_1}{dt} = K_{SI} I(P_0 - I) - K_{IR} I - K_{IS} I;$$

$$E_i = E_{i-1}(t - \tau_{E_{i-1}}), \ i = \overline{2, n};$$

$$I_1 = E_n(t - \tau_{E_n});$$

$$I_j = I_{j-1}(t - \tau_{I_{j-1}}), \ j = \overline{2, m};$$

$$\frac{dR}{dt} = K_{IR} I_m;$$

$$\frac{dF}{dt} = K_{IF} I_m;$$

$$\frac{dS}{dt} = K_{IS} I_m.$$

Системы уравнений других моделей построены аналогично.

SLBQRS [15] — в модель SEIR (SLBS) добавлено состояние выдерживания объектов в карантине Q (рис. 1, *ж*).

SIPS [10, 18] — учтены расходы машинных ресурсов (в частности, временных) для накладывания заплаток на уязвимости программных систем (рис. 1, *з*). Пунктиром показано состояние, которое по логике должно присутствовать, но в названии модели не отображено.

PSIDR (Progressive SIDR) [11] — данная модель отдельно рассматривает состояние детектирования *D* (обнаружения) злонамеренного кода и динамику реакции системы на выявленную опасность. Эту модель еще называют моделью с противодействием [9]. Процедура модели PSIDR двухэтапная. На первом этапе система работает, как модель SI, на втором этапе — как модель SIDR (рис. 1, *и*).

Эволюция рассмотренных моделей на начальных этапах происходила в одинаковой последовательности как для биологических, так и для компьютерных эпидемий. В дальнейшем различия физической сущности объектов привели к существенным отличиям в направлениях развития моделей (рис. 2).

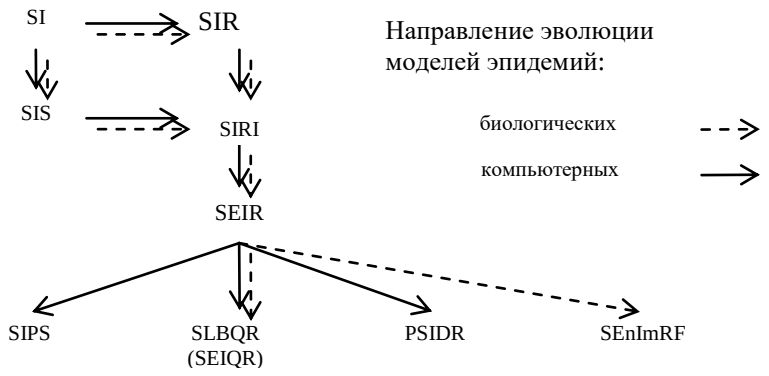


Рис. 2

3. Совершенствование существующих моделей эпидемий

3.1. Расширение набора типов состояний *S*. Некоторые авторы уже расширяли набор типов состояний *S*, но определяли их как принципиально новые *R* (Removed, Recovered) [14], D (Delay) [23] и не связывали между собой, хотя на самом деле все они являются частными случаями состояния *S*. Предлагается ввести такие подвиды состояния *S*: S_1 — восприимчивость к первичному заражению; S_2 — восприимчивость к заражению после, того как объект вылечен, но не получил иммунитет. В [14] обозначен как *R* (Removed, Recovered); S_3 — восприимчив к заражению после того, как объект излечен, получил иммунитет, но через некоторое время стал восприимчив к новой модификации инфекции. В [23] обозначен *D* (Delay), поскольку инфекция модифицируется с задержкой во времени.

3.2. Состояния *B* (Breaking-out) [15] (проявление заражения) и *D* (Detected) [9] (выявление заражения без активного противодействия). С точки зрения человеко-машинной системы наблюдения, эти состояния эквивалентны. Если заражение «проявилось» (*B*) для системы наблюдения, значит, оно «детектировано» (*D*). Вместо *B*, *D* предлагается использовать одно состояние *D*.

3.3. Состояние *I* предусматривает лечение за счет внешних ресурсов или самолечение за счет собственных ресурсов. Иначе объект из состояния *I* никогда не перейдет в другое состояние (кроме *F*). Для состояния *I* нужно рассматривать средства лечения для каждой стадии отдельно (I_1, I_2, ..., I_m) [9]. Если лечения нет, значит, оно равно нулю.

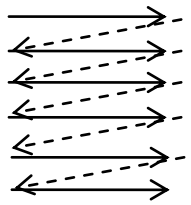
3.4. На начальной стадии проявления заражения система наблюдает и собирает информацию для наиболее эффективного противодействия. Значит, состояние *B* соответствует стадии I_1, а состояние *D* можно погрузить в одну из стадий (I_1, I_2, ..., I_m).

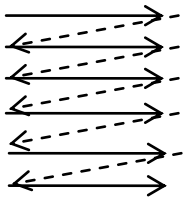
3.5. В состоянии *I* возможны карантин полный, частичный или лечение без карантина. *Q* (Quarantine) [15] — карантин (полная изоляция объекта). При этом функциональность и влияние средств противодействия заражению на функциональность системы равны нулю; *W* (Work) — ликвидация заражения без прекращения работы. В [18] рассматривалось состояние *P* (Patched) ликвидации обнаруженных уязвимостей без прекращения работы. Действия по ликвидации заражения расходуют функциональный ресурс системы, но заданный запас функциональной устойчивости может сохраняться.

Таким образом, вместо состояния *I* можно использовать состояния *Q*, *W* (какое-то одно или оба). Поскольку *I* имеет несколько стадий $I = \{I_1, I_2, ..., I_m\}$, состояния *Q*, *W* также имеют несколько стадий, которые описывают векторы такой же длины $Q = \{Q_1, Q_2, ..., Q_m\}$, , $W = \{W_1, W_2, ..., W_m\}$. По сравнению с состоянием *I*, здесь ситуация несколько сложнее, поскольку на каждой стадии может быть несколько этапов лечения. Тогда векторы *Q*, *W* нужно заменить матрицами (рис. 3, *а*)

$$Q = \begin{vmatrix} Q_1 \\ Q_2 \\ Q_3 \\ Q_4 \\ \vdots \\ Q_m \end{vmatrix} = \begin{vmatrix} q_{11} & q_{12} & q_{13} & q_{14} & \dots & 0 \\ q_{21} & q_{22} & 0 & 0 & \dots & 0 \\ q_{31} & q_{32} & q_{33} & q_{34} & \dots & q_{3r} \\ q_{41} & q_{42} & q_{43} & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ q_{m1} & 0 & 0 & 0 & \dots & 0 \end{vmatrix},$$

$$W = \begin{vmatrix} W_1 \\ W_2 \\ W_3 \\ W_4 \\ \vdots \\ W_m \end{vmatrix} = \begin{vmatrix} w_{11} & w_{12} & 0 & 0 & \dots & 0 \\ w_{21} & w_{22} & w_{23} & w_{24} & \dots & w_{2r} \\ w_{31} & w_{32} & w_{33} & w_{34} & \dots & w_{3r} \\ w_{41} & w_{42} & w_{43} & w_{44} & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ w_{m1} & w_{m2} & w_{m3} & 0 & \dots & 0 \end{vmatrix}.$$





а *б*

Рис. 3

В матрицах *Q*, *W* по вертикали расположены стадии заражения, а по горизонтали — этапы лечения для каждой стадии. Количество этапов лечения для каждой стадии разное. Кроме того, количество этапов лечения разное для лечения в карантине *Q* и без карантина *W*. Отдельные элементы матриц *Q*, *W* показывают количество объектов, которые находятся на соответствующем этапе лечения соответствующей стадии. При моделировании нужно последовательно проходить все состояния в каждой строке, затем переходить к началу следующей строки (рис. 3, *б*).

3.6. Обычно лечение проводится после того, как заражение уже проявилось *I*, или при формировании невосприимчивости объектов к заражению до начала эпидемии N_0. Добавим состояние N_2 (Not susceptible) — невосприимчивость к заражению вследствие профилактических мер Pre (Prevent), которые применяются по отношению к восприимчивым объектам *S* и объектам в латентном состоянии заражения *E*.

3.7. В существующих моделях эпидемий рассматриваются устойчивые результирующие состояния отдельных объектов. N_1 — невосприимчивость к заражению, которая существовала до начала эпидемии, R — вылеченный объект, который приобрел иммунитет, F — полностью утраченный (погибший) объект. В то же время реалии таковы, что большое количество объектов после заражения и лечения возвращаются к работе с пониженным запасом функциональной устойчивости. Для биологических эпидемий это — осложнение после болезней, которое может приводить к инвалидности. Но нужно жить, и люди работают в состоянии меньшей функциональности. Для компьютерных эпидемий это — ужесточение настроек систем защиты, которые расходуют дополнительные вычислительные ресурсы и мешают работать тем вычислительным ресурсам, которые остались.

Введем еще один набор устойчивых результирующих состояний для отдельных объектов после эпидемии: состояние частичной функциональности — V (inValid). Находящиеся в этом состоянии объекты нужно разделить на несколько групп по уровням остаточной функциональности V_1, V_2,..., V_k. Количество состояний k зависит от внешних условий, особенностей исследуемой системы и особенностей постановки задачи.

С учетом предложенных изменений все возможные состояния обобщены в таблице. Усовершенствованную общую модель эпидемиологического процесса представим в виде структурной VNF-модели (по первым буквам стационарных состояний, возникающих после окончания эпидемии; inValid, Nonsusceptible, Fatal) (рис. 4).

Таблица

Авторы, модели	Обозначения возможных состояний объектов ИС															
Обобщенные и предложенные в данной работе — VNF	P_0	N_0	S_1	S_2	S_3	E	n	B	D	I	m	Q_m	W_m	N_{1R}	F	V
Kermack, McKendrick, 1927, SIR																
Kephart, Whites, 1991, SIS																
Бароян, Рвачев, 1977, SEnImRF	*P*		*S X*			*E*	*n*			*IY*	*m*			*R*	*F*	
Cohen, 1985																
Garetto, Gong, Towsley, 2003, SIR			*S*							*I*				*M*		
Serazzi, Zanero, 2003, MSEIR		*M*	*S*			*E*				*I*				*R*		
Боев, 2004, SEIRF	*P*		*S*			*E*				*I*				*R*	*F*	
Боев, 2005, SEIR SEnImRF	*P*		*S X*			*E*	*n*			*I*	*m*			*R*	*F*	
Martcheva, 2005, SIS, SIR	*N*		*S*	*R*						*I*						
Britton, 2009, SIS, SIR, SEIR, SIRS			*S*			*E*				*I*				*R*		
Монахов, Груздева, Монахов 2010, SI, SIS, SIR, PSIDR			*S*			*E*			*D*	*I*				*R*		
Stollenwerk, Jansen, 2011, SIS, SIR, SIRI			*S*							*I*				*R*		
Климентьев, 2013, SI, SIS, SIR, SEIR, SIRS, PSIDR			*S*	*S*		*E*			*D*	*I*				*R*		
Yang, Yang, Wu, 2017, SLBS, SIPS			*S*	*S*				*B*		*I*			*P*			
Zhang, Wang, Ferrara, SEIQRS с задержками			*S*	*S*		*E*				*I*		*Q*				
Zhang, Song, 2017, SLBRS с задержками			*S*			*L*		*A*						*R*		
Umbreen, Mubasher, Nauman, Malik, 2018, SLBQRS			*S*	*S*		*L*		*B*				*Q*		*R*		
Onwubuoya, Akinuemi, Odabi, Odachi, 2018, SIRS	*N*		*S*	*R*						*I*				*A*		
Yao, Fu, Yang, Wang, Sheng, 2018, SIQVD			*S*		*D*					*I*		*Q*		*V*		
Champredon, Dushoff, Earn, 2018, SEIR			*S*			*E*				*I*				*R*		

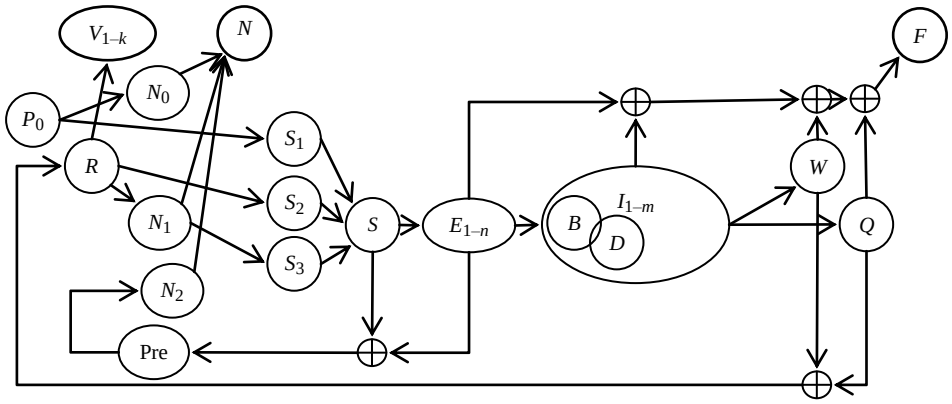


Рис. 4

3.8. Модель VNF опишем системой уравнений. Примем дополнительные обозначения: N, N_0, N_1, N_2 — количество объектов, невосприимчивых к заражению вследствие рассмотренных выше причин (без индексов — суммарное количество); S_1, S_2, S_3 — количество объектов, восприимчивых к заражению вследствие рассмотренных выше причин; W_j, Q_j — количество инфицированных объектов на разных стадиях, $j = \overline{1, m}$, при лечении без карантина и в карантине соответственно; V_j, R_j — количество объектов, вылеченных, получивших иммунитет, но оказавшихся в разных группах, $j = \overline{1, k}$, по уровню частичной потери функциональности и по результативности лечения соответственно. K_{IE}, K_{WR}, K_{QR}, K_{WF}, $K_{QF}, K_{SN}, K_{PS}, K_{RS}, K_{RN}, K_{NS}$; K_{IWj}, $j = \overline{1, m}$; K_{ENi}, $i = \overline{1, n}$; K_{RVj}, $j = \overline{1, k}$, — коэффициенты интенсивности переходов между различными состояниями. Первый индекс показывает начальное состояние, второй — конечное, третий — номер стадии периода или степень успешности лечения. Pre — функция профилактических мер по увеличению количества объектов, невосприимчивых к заражению; y_i, $i = \overline{1, n}$, — компоненты вектора всех возможных состояний объектов системы.

$$\frac{dE_1}{dt} = K_{IE} I (P_0 - I) - (K_{WR} W_m + K_{QR} Q_m) - (K_{WF} W_m + K_{QF} Q_m),$$

$$\frac{dR}{dt} = K_{WR} W_m + K_{QR} Q_m,$$

$$\frac{dF}{dt} = K_{WF} W_m + K_{QF} Q_m,$$

$$\frac{dN_2}{dt} = \mathrm{Pre}\left(S + \sum_{i=1}^{n} E_i \right) = K_{SN} S + \sum_{i=1}^{n} K_{ENi} E_i,$$

$$E_i = E_{i-1}(t - \tau_{E_{i-1}}), \quad i = \overline{2, n},$$

$$I_1 = E_n(t - \tau_{E_n}),$$

$$I_j = I_{j-1}(t - \tau_{I_{j-1}}), \quad j = \overline{2, m},$$

ISSN 0572-2691

$$S_1 = K_{PS} P_0,$$

$$N_0 = (1 - K_{PS}) P_0,$$

$$W_j = K_{IWj} I_j, \quad j = \overline{1, m},$$

$$Q_j = (1 - K_{IWj}) I_j, \quad j = \overline{1, m},$$

$$S_2 = K_{RS} R,$$

$$N_1 = K_{RN} R,$$

$$S_3 = K_{NS} N_1,$$

$$V_j = K_{RVj} R_j, \quad j = \overline{1, k},$$

$$I_j = W_j + Q_j, \quad j = \overline{1, m},$$

$$I = \sum_{j=1}^{m} I_j, \quad S = \sum_{i=1}^{3} S_i, \quad N = \sum_{i=0}^{2} N_i, \quad P_0 = \sum_{i=1}^{r} y_i.$$

Большинство существующих моделей эпидемий — частные случаи модели VNF. Например, модифицированная структурная модель Б.В. Боева [13, 24–26] (рис. 5). Здесь приняты дополнительные обозначения: K_S, K_E, K_F — коэффициенты восприимчивости к заражению, передачи заражения, изъятия из работы соответственно; $f(I, S, K_E)$ — логистическая зависимость заражения. Динамика изменения количества объектов ИС, находящихся в различных состояниях, для рассмотренной модели на примере эпидемии червя CRv1 (Code Red версия 1) [5] представлена на рис. 6 (P = 600000, Ks = 0,85, Ke = 8e – 08, Kr = 0,8, Tae = 1, Tai = 9).

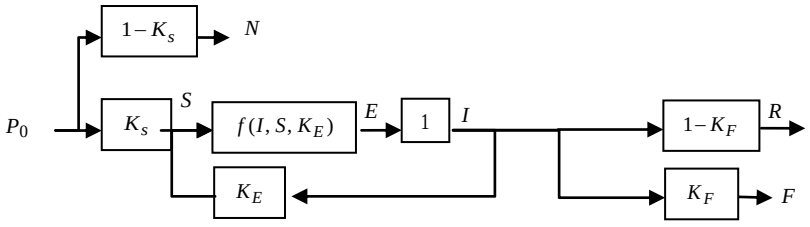


Рис. 5

Качественные картины динамики развития многих эпидемий, например CRv1, CRv2, SQL Slammer, похожи, но развиваются в своих масштабах времени. Наиболее типичным можно считать этап роста уровня заражения. Этот этап хорошо аппроксимируется логистической кривой и длится около $2T$, где T — постоянная логистической зависимости развития (для каждого случая эпидемий она имеет свою величину, в зависимости от вида заражения и состояния параметров системы защиты).

Этап роста числа инфицированных объектов качественно подобен для всех рассмотренных эпидемий. Момент начала этапа зависит от вида заражения и начального количества зараженных объектов. Чем больше объектов являются источниками заражения, тем быстрее начинается этап роста.

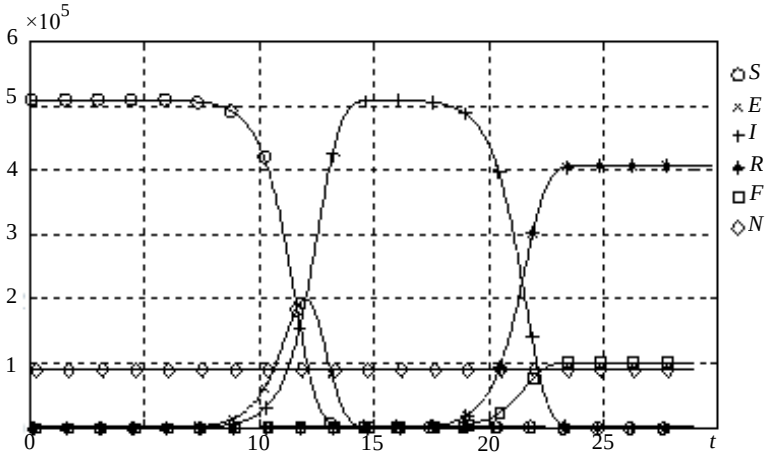


Рис. 6

Этап стабилизации на максимуме (этап начала лечения), по сравнению с этапом роста, более протяженный (у червей CRv1, CRv2 в несколько раз, у червя SQL Slammer — в несколько десятков или сотен раз). Чем раньше начинается и чем оперативнее лечение, тем меньше продолжительность этапа стабилизации.

4. Зависимость динамики процессов развития от параметров модели

Главным практическим результатом моделирования является «колоколообразная» зависимость количества зараженных объектов, амплитуда которой (высота пика эпидемии) определяет уровень эпидемической опасности. Под эпидемией понимаем состояние, когда процент выведенных из строя объектов превышает определенную величину. В техническом смысле это величина, при превышении которой полностью теряет нормальную работоспособность информационная инфраструктура рассматриваемой бизнес-области (предприятие, организация, отрасль). Высота пика эпидемии и другие характеристики динамики эпидемии в основном зависят от коэффициентов восприимчивости к заражению K_S и передачи заражения K_e. Если известен уровень эпидемического пика и его зависимость от Ks, Ke, то можно пытаться удержать управляющие параметры Ks, Ke в безопасных пределах.

Высота пика эпидемии CRv1 существенно зависит от коэффициента восприимчивости к заражению K_S, который непосредственно влияет на количество объектов, принципиально невосприимчивых к заражению (рис. 7, *а*; w=600000, K_e = 8e – 08, K_r = 0,8, Ta_e = 1, Ta_i = 9). Чем меньше K_S, тем меньше высота пика эпидемии и тем позже начинается этап роста заражения, что дает временной запас для принятия дополнительных мер защиты.

Практические пути уменьшения K_S.

- Полное отключение от сети (перевод в автономный режим) и запрет использования внешних носителей информации.
- Отключение от компьютерной сети на большую часть рабочего времени и эффективное противодействие возможному заражению в короткие периоды подключения к сети.
- Резервирование информации.

• Установка программных и программно-аппаратных средств противодействия злонамеренному коду с высоким уровнем защиты.

• Величина коэффициента передачи заражения K_e практически не влияет на величину пика эпидемии (рис. 7, *б*; w=600000, K_s=0,85, K_r=0,8, Ta_e=1, Ta_i=9), но чем меньше K_e, тем позже начинается этап роста заражения, что дает возможность успеть противодействовать заражению.

Практические пути уменьшения K_e.

• Уменьшение количества соединений в системе при постоянном количестве узлов.

• Установка в узлах, отвечающих за пересылку информации, программных и программно-аппаратных средств противодействия злонамеренному коду с высоким уровнем защиты.

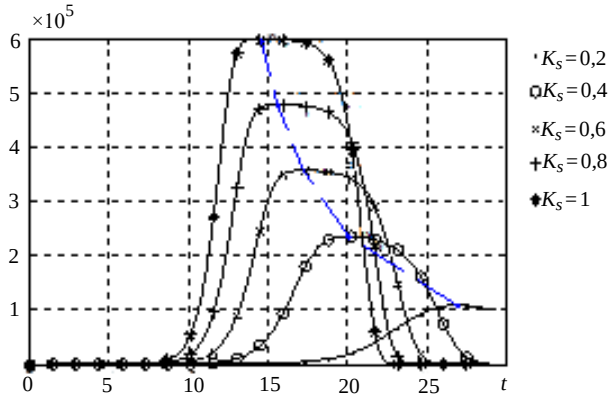
• Увеличение времени обработки сообщений при пересылке информации. Это ухудшает функциональность, но позволяет более тщательно проверить код в условиях микрокарантина.

• Пересылка информации большими пакетами с тщательным контролем возможного заражения.

• Для атак «нулевого дня» — использование IDS (Intrusion Detection System), которые выявляют сам факт атаки по признакам нетипичного поведения системы, даже если атака такого вида состоялась впервые. Далее выполняется блокирование возможных путей распространения заражения, а зараженная часть системы переводится в режим карантина, изучается, анализируется, лечится.

• Пересылка информации исключительно через узлы с высокой степенью доверия (в частности, имеющие специальные инструменты защиты информации) и др.

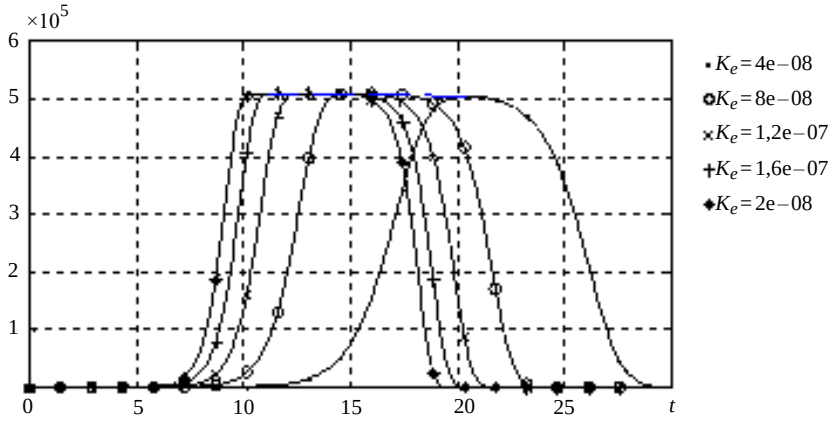
Как видим, одним из самых репрезентативных показателей опасности является высота пика эпидемии. Для увеличения эффективности противодействия эпидемии нужно одновременное управление всеми факторами влияния на процесс. В данном случае это — одновременное управление уровнем опасности через коэффициенты восприимчивости к заражению K_S и передачи заражения K_e. Вид зависимости высоты пика эпидемии от параметров K_S и K_e представлен на рис. 8, *а*. В большей части области допустимых значений высота пика эпидемии зависит только от K_S. Но в зоне наименьших величин указанных параметров, соответствующей небольшим величинам высоты пика эпидемии, оба параметра важны для получения высоты пика на наименьшем возможном уровне. Данная закономерность характерна для CRv1, но совершенно не обязательна, например, для SQL Slammer.



а

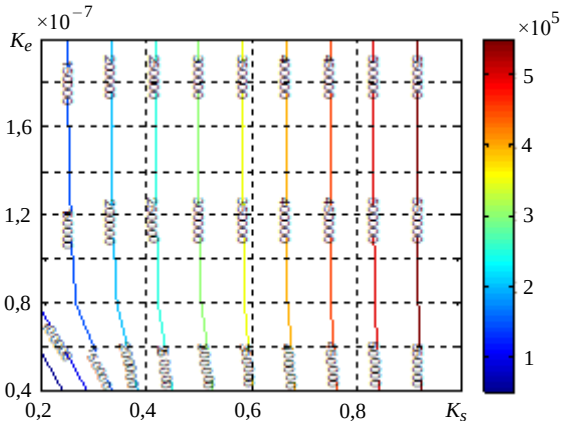
Рис. 7

Продолжение рис. 7

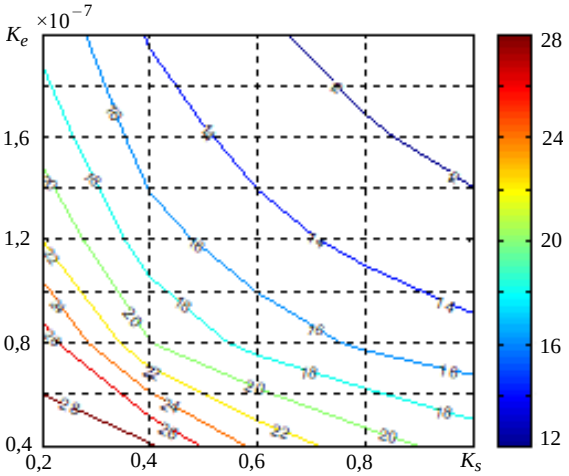


б

Для обеспечения резерва времени на своевременное принятие решения актуальным является управление временем достижения пика эпидемии, которое также зависит от K_S и K_e (рис. 8, *б*). В этом случае оба параметра одинаково эффективны по управлению временем достижения пика эпидемии.



а



б

Рис. 8

ISSN 0572-2691

Заключение

1. Уточнены классификации моделей компьютерных эпидемий, в частности классификация возможных состояний объектов информационной системы во время эпидемии.

2. Предложены пути совершенствования существующего множества возможных состояний объектов информационной системы и на основании этого усовершенствованы структурно-логическая и математическая модели компьютерных эпидемий.

3. Моделирование показало высокую степень качественного подобия процессов развития компьютерных эпидемий биологическим при различных видах заражения, в часности CRv1, CRv2, Slammer.

4. Рассмотрена возможность управления уровнем опасности эпидемии с помощью управляющих параметров — коэффициента восприимчивости к заражению и коэффициента передачи заражения.

5. Предложено усовершенствование модели в целях ее использования для моделирования уровня функциональности информационной системы.

6. Направлениями дальнейших исследований является апробация модели на различных видах заражений и усовершенствование в направлении моделирования функциональной устойчивости информационной системы.

7. Еще одним направлением дальнейших исследований является более детальный учет топологии компьютерных сетей.

О.С. Бичков, В. Новотна, В.Л. Шевченко, А.В. Шевченко

ВДОСКОНАЛЕННЯ МОДЕЛІ КОМП'ЮТЕРНИХ ЕПІДЕМІЙ НА ОСНОВІ РОЗШИРЕННЯ БЕЗЛІЧІ МОЖЛИВИХ СТАНІВ ОБ'ЄКТІВ ІНФОРМАЦІЙНОЇ СИСТЕМИ

Комп'ютерні атаки на інформаційні системи сьогодні набули глобального епідеміологічного характеру. Для ефективної протидії необхідно прогнозувати розвиток атак. Актуальним є вдосконалення моделей комп'ютерних епідемій і визначення керуючих параметрів, які утримують епідемію в безпечних межах. Мета статті — удосконалення існуючих моделей комп'ютерних епідемій шляхом виявлення неврахованих станів об'єктів інформаційних систем. Розглянуто та уточнено класифікацію можливих станів атакованих об'єктів інформаційних систем. Розширено набір типів станів сприйнятливості та несприйнятливості до зараження, враховано вплив профілактичних заходів. Уточнено облік станів появи і детектування ознак зараження. Деталізовано облік різних стадій інфікованого стану, лікування в карантині і без карантину. Введено новий набір станів об'єктів після епідемії — часткова функціональність різного ступеня. Об'єкти, що знаходяться в цьому стані, розділено на кілька груп за рівнями залишкової функціональності. Кількість станів залежить від зовнішніх умов, особливостей досліджуваної системи та особливостей постановки завдання. Розглянуто і уточнено класифікацію моделей комп'ютерних епідемій SI, SI exp, SI SL, SIS, SIR, SIRI, SEIR, SEnImRF, SLBQRS, PSIDR. Розглянуто подібність біологічних та комп'ютерних епідемій. Загальна модель епідеміологічного процесу вдосконалена у вигляді структурної VNF-моделі. Показано, що більшість існуючих моделей епідемій є окремими випадками моделі VNF. Удосконалено та апробовано структурно-логічну і математичну моделі комп'ютерних епідемій на прикладі епідемії хробака Code Red CRv1. Встановлено, що якісні картини динаміки розвитку багатьох епідемій, наприклад CRv1, CRv2, SQL Slammer, схожі, але розвиваються в своїх масштабах часу. Найбільш типовим можна вважати етап зростання рівня зараження, який добре апроксимується логістичною кривою. Запропоновано керування рівнем небезпеки епідемії через коефіцієнт сприйнятливості до зараження і коефіцієнт передачі зараження.

Ключові слова: комп'ютерні епідемії, модель, керування, стан об'єкта.

A.S. Bychkov, V. Novotna, V.L. Shevchenko, A.V. Shevchenko

IMPROVEMENT OF THE MODEL OF COMPUTER EPIDEMICS ON THE BASIS OF EXPANDING THE SET OF POSSIBLE STATES OF THE INFORMATION SYSTEM OBJECTS

Computer attacks on information systems today have acquired a global epidemiological character. For effective counteraction, it is necessary to predict the development of attacks. It is relevant to improve the models of computer epidemics and determine the control parameters that keep the epidemic within safe limits. The purpose of the article: improving existing models of computer epidemics by identifying unaccounted states of objects of information systems. The paper considers and refines the classification of possible states of attacked objects of information systems. The set of types of states of susceptibility and immunity to infection has been expanded, the influence of preventive measures has been taken into account. The account of the appearance and detection of infection signs has been refined. A detailed account of the various stages of an infected condition, treatment in quarantine and treatment without quarantine is detailed. A new set of state of objects after the epidemic has been introduced — partial functionality of varying degrees. Objects in this state are divided into several groups according to the levels of residual functionality. The number of states depends on external conditions, the characteristics of the system under study, and the characteristics of the problem statement. The classification of computer epidemic models SI, SI exp, SI SL, SIS, SIR, SIRI, SEIR, SEnImRF, SLBQRS, PSIDR is considered and refined. The similarity of biological and computer epidemics is considered. The general model of the epidemiological process is improved as a structural VNF model. It is shown that most existing epidemic models are particular cases of the VNF model. The structural-logical and mathematical models of computer epidemics are improved and tested using the Code Red CRv1 worm epidemic as an example. It has been established that qualitative pictures of the dynamics of the development of many epidemics, for example, CRv1, CRv2, SQL Slammer, are similar, but they are developing in their own time scales. The most typical stage is the growth of the level of infection. This stage is well approximated by the logistic curve. The management of the epidemic hazard level through the coefficient of susceptibility to infection and the transmission coefficient of infection is proposed.

Keywords: computer epidemics, model, management, state of an object.

1. Petrov P., Dimitrov G., Ivanov S. A comparative study on websecurity technologies Used in Irish and Finnish banks. *18 International Multidisciplinary Scientific Geoconference SGEM 2018: Conference Proceedings*. 2018. Albena, Bulgaria : **18**. Informatics, Geoinformatics a. remote sensing. N 2.1. Informatics, Sofia : STEF92 Technology Ltd., 2018. **18**, N 2.1. P. 3–10.
2. Cohen F. Computer viruses. PhD thesis. University of Southern California. 1985. 152 p.
3. Kephart J.O., Whites S.R. Directed-graph epidemical models of computer viruses. *Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy*. 1991. P. 343–358.
4. Garetto M., Gong W., Towsley D. Modeling malware spreading dynamics. *IEEE INFOCOM 2003.* www.ieee-infocom.org/2003/papers/46_01.PDF (accessed 23 March 2017).
5. Staniford S., Paxson V., Weaver N. How to own the internet in your spare time. *Proceedings of the 11th USENIX Security Symposium (Security '02).* 2002. P. 149–167.
6. Moore D., Shannon C. The spread of the code-red worm (CRv2). *Офіційний сайт Центру прикладного аналізу Інтернет даних CAIDA.* https://www.caida.org/research/security/code-red/coderedv2_analysis.xml. 2001.
7. Moor D., Shannon C., Brown J. Code-red: a case study on the spread and victims of an internet worm. *Proceedings of the ACM SIGCOMM/USENIX Internet Measurement Workshop*. 2002. P. 273–284.

8. Serazzi G., Zanero S. Computer virus propagation models. Calzarossa M.C., Gelenbe E. (eds) *Performance Tools and Applications to Networked Systems. MASCOTS 2003. Lecture Notes in Computer Science*. 2003. **2965**. P. 26–50. https://doi.org/10.1007/978-3-540-24663-3_2
9. Климентьев К.Е. Компьютерные вирусы и антивирусы: взгляд программиста. М. : ДМК Пресс, 2013. 656 с.
10. Chunming Zhang. Global behavior of a computer virus propagation model on multilayer networks. *Hindawi. Security and Communication Networks.* 2018. **2018**, Art.ID 2153195. P. 1–9. https://doi.org/10.1155/2018/2153195.
11. Leveille J. Epidemic spreading in technological networks. 2002. 100 p. www.hpl.hp.com/ techreports /2002/HPL-2002-287.pdf (accessed 23 March 2017)
12. Nowzari Cameron, Victor M. Preciado, George J. Pappas. Analysis and control of epidemics: a survey of spreading processes on complex networks. *IEEE Control Systems 36.1*. 2016. P. 26–46.
13. Боев Б.В., Макаров В.В. Геоинформационные системы и эпидемии гриппа. *Ветеринарная патология.* 2004. № 3 (10). С. 51–59. http://elibrary.ru/item.asp?id=9165685 (accessed 23 March 2017)
14. Onwubuoya C., Nwanze D.E., Erejuwa J.S., Akinyemi S.T. An approximate solution of a computer virus model with antivirus using modified differential transform method. *International Journal of Engineering Research (IJERT)*. 2018. **7**, N 04. P. 154–161. www.ijert.org
15. Umbreen F., Mubasher A., Nauman Ah., Muhammad R.M. Numerical modeling of susceptible latent breaking-out quarantine computer virus epidemic dynamic. *Heliyon.* 2018. **4**, e00631. P. 1–21. doi: 10.1016/j.heliyon.2018.e00631
16. Бароян О.В., Рвачев Л.А., Иванников Ю.Г. Моделирование и прогнозирование эпидемий гриппа для территории СССР. М. : ИЭМ. им. Н.Ф. Гамалеи, 1977. 546 с.
17. Zizhen Zhang, Limin Song. Dynamics of a computer virus propagation model with delays and graded infection rate. *Hindawi. Advances in Mathematical Physics.* 2017. **2017**, Article ID 4514935. P. 1–13. https://doi.org/10.1155/2017/4514935
18. Yang L.-X., Yang X., Wu Y. The impact of patch forwading on the prevalence of computer virus: a theoretical assessment approach. *Applied Mathematical Modelling*. 2017. **43**. P. 110–125.
19. Kermack W.O., McKendrick A.G. A contribution to the mathematical theory of epidemics. *Proc. Roy. Soc. Lond. A.* 1927. **115**. P. 700–721.
20. Вьюн В.И., Еременко Т.К., Кузьменко Г.Е., Михненко Ю.А. Об одном подходе к прогнозированию эпидемиологической обстановки по гриппу-ОРВИ с использованием временных рядов. *Математичні машини і системи.* 2011. № 2. С. 131–136.
21. Соловьйов С.О., Терещенко І.О., Дзюблик І.В. Математичне моделювання і прогнозування захворюваності на ротавірусну інфекцію серед дітей до п'яти років в Україні. *Медична інформатика та інженерія.* 2012. № 1. С. 23–29.
22. Stollenwerk N., Jansen V. Population biology and criticality. *From critical birth-death processes to self-organized criticality in mutation pathogen system.* London : Imperial College Press. 2011. 224 p.
23. Yu Yao, Qiang Fu, Wei Yang, Ying Wang, Chuan Sheng. An epidemic model of computer worms with time delay and variable infection rate. *Hindawi. Security and Communication Networks.* 2018. **2018**, Art.ID 9756982. P. 1–11. https://doi.org/10.1155/2018/9756982
24. Shevchenko A., Shcheblanin J., Shevchenko V. The epidemiological approach to prognosis and management of information incidents. *Системи обробки інформації.* 2017. № 5 (151). С. 145–150. http://www.hups.mil.gov.ua/periodic-app/journal/soi/2017/5
25. Shevchenko A., Shevchenko V. The epidemiological approach to information security incidents forecasting for decision making systems. *13-th International Conference Perspective Technologies and Methods in MEMS Design (MEMSTECH). Proceeding.* Polyana, April 20-23, 2017. P. 174–177. http://ieeexplore.ieee.org/document/7937561/ DOI: 10.1109/ MEMSTECH. 2017.7937561.
26. Гепко А.Л., Шевченко А.В. Математична модель прогнозування динаміки епідемій. *Профілактична медицина.* № 3 (15). С. 3–6.

Получено 20.06.2019
После доработки 13.08.2019