УДК 004.942:004.49:004.056.57

А.С. Бычков, Г.П. Димитров, В.Л. Шевченко, А.В. Шевченко

СОВЕРШЕНСТВОВАНИЕ МОДЕЛИ КОМПЬЮТЕРНЫХ ЭПИДЕМИЙ ПУТЕМ ОЦЕНИВАНИЯ ФУНКЦИОНАЛЬНОЙ УСТОЙЧИВОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ

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

Введение

Рост числа инцидентов в сфере информационной безопасности как минимум вдвое превышает темпы роста мобильного рынка [1, 2]. Целью постоянных компьютерных атак являются информационные системы (ИС) всех секторов экономики, в частности государственных учреждений, силовых ведомств, бизнеса всех уровней, сферы здравоохранения, банковского сектора [3]. Особенно опасно то, что около 70 % атак остаются невыявленными [2]. Почти нормой становится функционирование ИС в условиях воздействия инцидентов информационной безопасности. Для эффективного противодействия инцидентам необходимо четко понимать, как меняется функциональная устойчивость ИС во времени. Для этого необходимо прогнозировать динамику ее изменения во времени. Поэтому совершенствование моделей динамики функциональной устойчивости информационных систем в условиях информационных инцидентов эпидемиологического масштаба является актуальной задачей. Функциональная устойчивость [4] — это способность «системы выполнять свои функции в течение заданного интервала времени при условии воздействия на нее эксплуатационных отказов, преднамеренных повреждений, вмешательств в обмен и обработку информации и ошибок персонала». Функциональность является близким понятием и отражает набор функций, которые выполняет система. Численно функциональность можно определить как часть функций или суммарный полезный эффект от доступных функций системы, которые система сохранила на текущий момент, несмотря на вредные воздействия.

Цель статьи — усовершенствовать существующие модели компьютерных эпидемий путем оценивания функциональной устойчивости информационной системы.

1. Обобщенная математическая постановка задачи

1. Модель динамики изменения состояний Y информационной системы $\frac{dY}{dt} = F(Y).$

Модель функциональной устойчивости Ф информационной системы на основе исходных данных модели динамики состояний $\Phi = \Phi(Y).$

2. Ограничения на фазовые координаты состояний $Y < Y_{zad}$.

Ограничения на функциональность системы $\Phi > \Phi_{zad}$.

3. Критерий качества $\Phi \to \max$.

При необходимости критерий можно перевести в ограничения $\Phi > \Phi_{zad}$.

2. Обобщение существующих моделей компьютерных эпидемий

Компьютерные эпидемии имеют много общего с медицинскими эпидемиями. Поэтому математические модели компьютерных эпидемий изначально базировались на моделях медицинских эпидемий [5, 6]. В работе [7] авторами обобщены существующие и введены новые обозначения для характеристики возможных состояний объектов информационной системы в условиях компьютерной эпидемии. Представленные ниже переменные обозначают количество объектов информационной системы, которые находятся в конкретном состоянии. Переменные с индексами обозначают количество объектов, находящихся на отдельных стадиях заражения, лечения, в подвидах отдельных родственных состояний. Переменные без индексов — суммарное количество объектов в описываемом состоянии. Приведенные ниже обозначения использованы в формулах, схемах, а также при указании видов моделей эпидемий.

Рассмотрим обозначения возможных состояний объектов информационной системы: P — суммарное количество всех объектов; N, N_0, N_1, N_2 — количество объектов, невосприимчивых к заражению; N_0 — невосприимчивые до начала эпидемии; N_1 или R — те, что получили иммунитет после лечения; индекс при R_j обозначает степень успешности лечения; N_2 — невосприимчивость, сформированная после начала эпидемии; S, S_1, S_2, S_3 — количество объектов, восприимчивых к заражению; S_1 — восприимчивость к первичному заражению; S_2 — восприимчивость к повторному заражению той же инфекцией; S_3 — восприимчивость вылеченного объекта к заражению новой модификацией инфекции; E — латентный период; E_i — разные стадии, $i = \overline{1, n}$, латентного периода; n — количество стадий латентного периода; B — заражение проявилось, но система защиты его еще не выявила; D — заражение выявлено, но противодействие еще не началось; I — объект активно заражает другие объекты; I_j — разные стадии, $j = \overline{1, m}$, активного периода; m — количество стадий заражения; Q, W — объекты в карантине и объекты, проходящие лечение без прекращения работы; Q_j, W_j — разные стадии, $j = \overline{1, m}$, лечения в карантине и без карантина; F — безвозвратно утраченные объекты; V, V_j — количество вылеченных объектов в группах, $j = \overline{1, k}$, с разным уровнем остаточной функциональности; $\tau_{E_{i-1}}$ — длительность разных стадий, $i = \overline{1, n}$, латентного периода заражения; $\tau_{I_{j-1}}$ — длительность разных стадий, $j = \overline{1, m}$, активного периода заражения; K_{SI}, K_{IS}, K_{IR}, K_{IF}, 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 невосприимчивых объектов; y_i, $i = \overline{1, n}$, — компоненты вектора всех возможных состояний объектов системы.

Для рассмотренных моделей можно записать вектор состояния ИС в виде $Y = \{N, S, E, I, B, D, R, Q, W, F...\}$ или в обозначениях с цифровыми индексами $Y = \{y_1, y_2, ..., y_r\}$.

В [7] сделан обзор основных видов моделей компьютерных эпидемий: SI (SI exp, SI SL), SIS [8], SIR [8–10], SIR(t) [11], SIRI [12], SEIR (SLBS) [13], SEnImRF [14], SLBQRS [15], SIPS [13], PSIDR [16]. Во всех рассмотренных моделях переходы между состояниями описывают уравнения Колмогорова в виде системы обыкновенных дифференциальных уравнений

$$\frac{dY}{dt} = F(Y).$$

Здесь $F(Y)$ — правые части дифференциальных уравнений в матричном виде. Дополнительным условием является неизменное количество суммы объектов во всех возможных состояниях в любой момент времени

$$P = \sum_{i=1}^{r} y_i.$$

Общую модель функциональной устойчивости ИС с учетом динамики изменения состояния объектов ИС в условиях компьютерных инцидентов опишем системой уравнений модели VNF [7]

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3. Модель функциональной устойчивости информационной системы

Реалии таковы, что большое количество объектов после заражения и лечения возвращаются к работе с пониженным запасом функциональности (функциональной устойчивости). Для биологических эпидемий это — осложнение после болезни, 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 мощности и мешают работать тем вычислительным ресурсам, которые остались.

Принципиальное отличие модели VNF заключается в том, что она в качестве критерия качества оценивает не только количество незараженных объектов *N*, *S*, как это делают обычно другие модели эпидемий, но и функциональность информационной системы в целом, с учетом того, что свой вклад в функциональность, кроме незараженных объектов *N*, *S*, могут вносить в определенном (меньшем) объеме также объекты, инфицированные на разных стадиях заражения $E_1 - n$, *B*, *D*, $I_1 - m$ ($W_1 - m$, $Q_1 - m$), и объекты, которые вылечены, но потеряли часть своей функциональности *V* с учетом уровня остаточной функциональности V_1, V_2, ..., V_k.

Для упрощения математической записи дальнейших выкладок представим дополнительные обозначения (синонимы) для возможных состояний объектов (табл. 1). Введем весовой коэффициент b_i, который соответствует части остатка функциональности для каждого состояния y_i. Например, для состояния *F* коэффициент остатка функциональности равен нулю, поскольку объект полностью и навсегда потерял свою функциональность. Для объектов, которые находятся в разных состояниях отсутствия заражения N_0, N_1, S_0, S_2, S_3, т.е. сохраняют полную функциональность, $b_i = 1$.

Таблица 1

Традиционные обозначения количества объектов в различных состояниях	N_0	S_1	S_2	S_3	$E_1 - n$	B	D	$Q_1 - m$	$W_1 - m$	$\frac{N_1}{R}$	F	V_k
Синонимы (новые) обозначения количества объектов в различных состояниях	y_1	y_2	y_3	y_4	y_5	y_6	y_7	y_8	y_9	y_{10}	y_{11}	y_{12}
Уровень остатка функциональности	b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8	b_9	b_{10}	b_{11}	b_{12}

Для всех остальных состояний b_i принимает значения от 0 до 1. При этом состояния $E_1 - n$, $Q_1 - m$, $W_1 - m$ ($n > 1, m > 1$) могут включать несколько составляющих. В таком случае добавляется соответствующее количество дополнительных переменных y_i, для каждой из которых определяется свой коэффициент функциональности b_i. Эти составляющие соответствуют различным состояниям и условиям заражения, которые, соответственно, сохраняют разный уровень функциональности. Общее выражение для функциональности информационной системы имеет вид

$$\Phi = \sum_{i=1}^{w} b_i y_i; \quad 0 \le b_i \le 1,$$

где w — количество состояний, влияющих на функциональность. Соответствующая логическая структура обработки данных приведена на рис. 1.

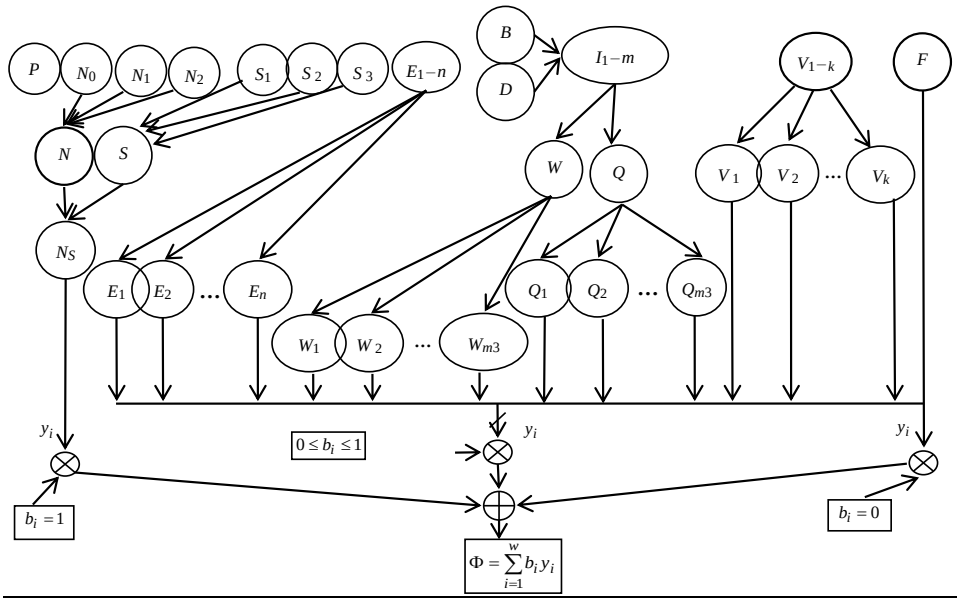


Рис. 1

Как известно, модели компьютерных эпидемий получены путем адаптации моделей биологических эпидемий к особенностям компьютерных объектов. С возникновением модели VNF появилась возможность улучшения моделей биологических эпидемий путем обратной адаптации моделей компьютерных эпидемий к особенностям биологических объектов. Логика взаимных трансформаций между биологическими и компьютерными моделями эпидемий представлена на рис. 2.

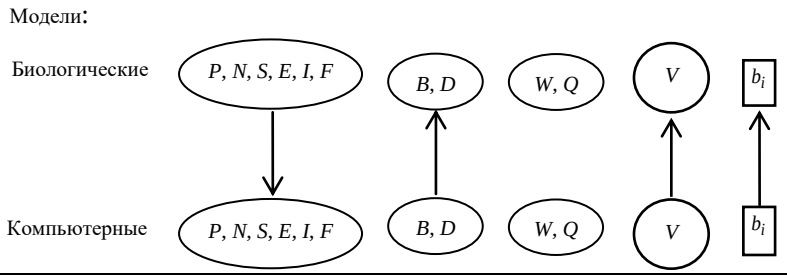


Рис. 2

Сначала состояния *P, N, S, E, I, F* были предложены в биологических моделях эпидемий, затем адаптированы для моделей компьютерных эпидемий. Состояния *B, D*, наоборот, сначала появились в моделях компьютерных эпидемий, а затем в биологических. Состояния *W, Q* появились в моделях компьютерных и биологических эпидемий практически независимо друг от друга. На рис. 2 жирными линиями и буквами показаны усовершенствования, которые предложены авторами данной работы. Состояние *V* [7] и использование весовых коэффициентов b_i для вычисления функциональности (функциональной устойчивости) системы первоначально представлены для моделей компьютерных эпидемий, а уже потом предложено использовать их также для моделей биологических эпидемий.

4. Моделирование функциональной устойчивости

Принципиальная разница в использовании ресурсов при компьютерных эпидемиях, в отличие от биологических, заключается в том, что больных людей работать не заставляют. Но несмотря на инфицированное состояние техника обычно работает до тех пор, пока это не становится слишком опасным или специалист не

примет соответствующее решение по кибербезопасности. Даже в зараженном состоянии работа вычислительной техники позволяет 1) выполнять основные штатные функциональные задачи; 2) бороться с заражением на автономном и сетевом уровнях. Поэтому вопрос оценки функциональности зараженной техники очень актуален.

В описываемом варианте модели эпидемий в качестве возможных состояний объектов рассмотрим следующие: *S*, *E*, *I*, *R*, *F*, *N*.

Матрица-строка общего состояния системы в нотации МАТЛАБ имеет вид

$$Y = [S\ E\ I\ R\ F\ N].$$

Традиционный подход. При планировании доступной функциональности обычно из числа трудоспособных объектов исключают только потерянные навсегда *F* и зараженные, которые находятся в активном состоянии заражения *I*. Другими словами, матрица-строка коэффициентов функциональности состояний имеет вид

$$B1 = [1\ 1\ 0\ 1\ 0\ 1].$$

Выражение для функциональной устойчивости системы выглядит так:

$$FS1 = \frac{1}{P}\sum_{i=1}^{6} B1_i\, y_i.$$

Усовершенствованный подход. На самом деле большинство объектов системы не имеют 100 % функциональности.

1. Объекты в латентном состоянии *E*. Даже если они не заражают другие объекты, часть своей функциональности они уже потеряли в результате заражения.

2. Объекты в активно зараженном состоянии *I*. Теряют большую часть своей функциональности. Но не всю. Возможно, именно эта доля сохраненной функциональности будет последней каплей, которая позволит выполнить важные штатные или нештатные задачи по противодействию эпидемии.

3. Объекты, невосприимчивые к заражению *N*. За все надо платить. Платой за их невосприимчивость к заражению является расход большой доли машинных ресурсов (и доли функциональности) на поддержку высокого уровня защищенности. Если невосприимчивость достигается отключением от сети, снижение функциональности связано с потерей сетевого доступа.

Матрица-строка коэффициентов функциональности состояний для сетевой ИС в условиях рассмотренных компьютерных эпидемий принимает вид

$$B2 = [1\ 0{,}5\ 0{,}2\ 1\ 0\ 0{,}8].$$

Значения матрицы *B*2 могут быть постоянными или изменяться во времени. Исходя из скоротечности компьютерных инцидентов, в большинстве случаев значения матрицы *B*2 можно считать постоянными. Значения матрицы *B2* зависят от особенностей 1) построения информационной системы; 2) набора функций информационной системы; 3) построения системы защиты от атак и ошибок программного обеспечения; 4) внешних условий; и т.п.

Выражение для функциональной устойчивости системы принимает вид

$$FS2 = \frac{1}{P}\sum_{i=1}^{6} B2_i\, y_i.$$

Для сравнения традиционного и усовершенствованного подходов оценки функциональности систем введем меру — погрешность оценки функциональности

$$\Delta FS = FS2 - FS1.$$

Величины $\Delta FS, FS1, FS2$ измеряем в процентах. Если ΔFS больше нуля, значит, традиционный подход дает заниженные показатели функциональности. Если меньше нуля, то завышенные. И то, и другое плохо, потому что вводит в заблуждение проектировщика и администратора информационной системы при оценке доступной функциональности на разных этапах планирования противодействия атакам. Проверка работоспособности предложенной модели функциональности проведена на примере моделирования эпидемий компьютерных червей CodeRed CRv1, CRv2, SQL Slammer и эпидемии гриппа в Украине.

Для этого в общей VNF-модели исключены неактуальные состояния по аналогии с модифицированной структурной моделью Б.В. Боева [17, 18]. В качестве наиболее значимых факторов влияния на функциональную устойчивость ИС выявлены коэффициент восприимчивости к заражению K_s и коэффициент передачи заражения K_e. Далее промоделированы показатели функциональной устойчивости $\Delta FS, FS1, FS2$ при изменениях коэффициентов K_s и K_e во всем диапазоне допустимых значений от 0 до 1.

В случае эпидемии CRv1 до этапа роста традиционный подход дал несколько завышенные показатели функциональности системы (рис. 3, *а*). Это связано с тем, что не учтены ресурсы, потраченные на защиту от атак. При проектировании на базе системного подхода в большинстве случаев избегают такой погрешности. К тому же ее величина не превышает 2–3 %. Поэтому такая погрешность не является критической.

Что касается этапа роста, традиционный подход сначала завысил показатели функциональности почти на 16 %, а затем занизил их почти на 16 %. На всем этапе лечения (этап стабилизации на максимуме) традиционный подход занизил функциональность на 16 %, что особенно критично для качества планирования ресурсов на противодействие заражению, которое уже произошло.

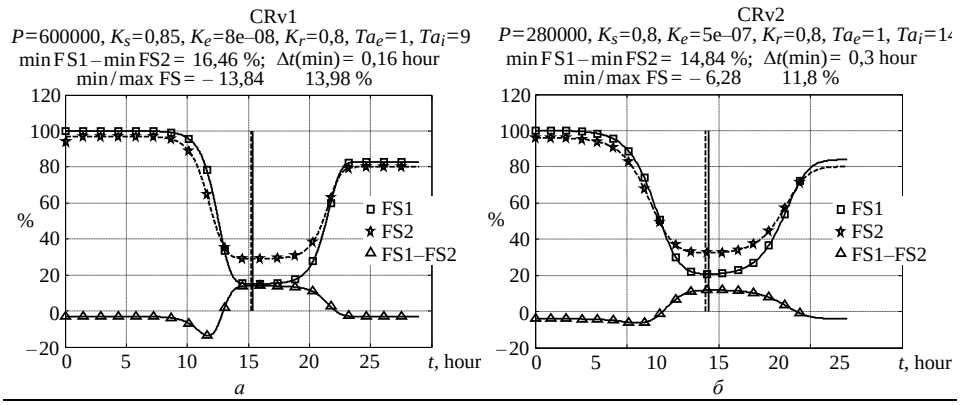


Рис. 3

Аналогичная качественная картина изменения погрешностей оценок функциональности наблюдается при моделировании эпидемий CRv2 и SQL Slammer (рис. 3, *б*, 4, *а*). Но есть численные различия. До этапа роста ΔFS = – 3 % (завышение $FS1$), на этапе роста ΔFS = – 3 – +10 % (сначала завышение, затем занижение $FS1$), на этапе лечения ΔFS = + 10 % (занижение $FS1$).

Принципиально качественное различие наблюдается для эпидемии гриппа (рис. 4, *б*). До этапа роста $\Delta FS = -11\ \%$, на этапе роста $\Delta FS = -13 - -4\ \%$, на этапе лечения $\Delta FS = -10 - -4\ \%$.

Другими словами, на всех этапах наблюдается завышение $FS1$. Это связано с тем, что 1) доля восприимчивых к заражению объектов в биологических эпидемиях намного выше; 2) массовое лечение начато гораздо раньше (уже во время этапа роста).

В [17, 18] показано, что величина пика эпидемии и время его достижения существенно зависят от параметров модели K_s, K_e. Аналогичным образом исследуем зависимость погрешности оценки функциональной устойчивости ΔFS от параметров K_s, K_e (рис. 5–7 — эпидемии ИС, рис. 8 — эпидемия гриппа).

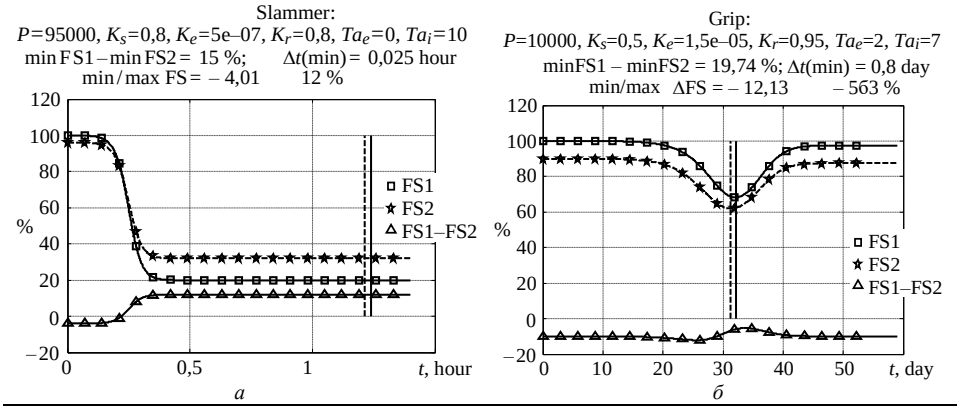


Рис. 4

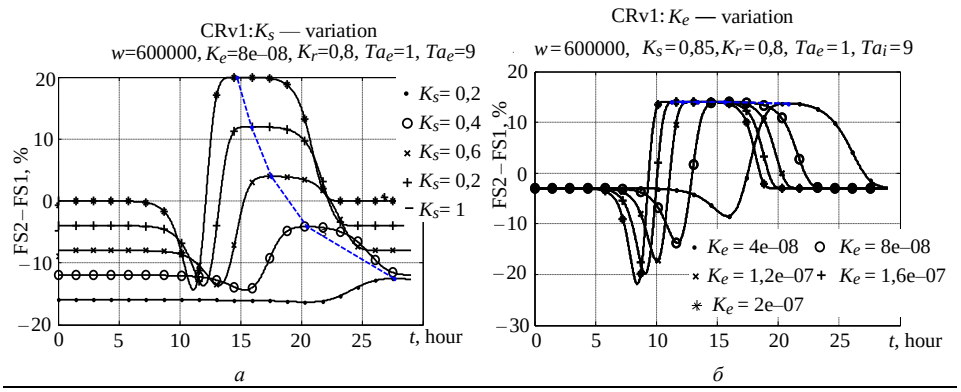


Рис. 5

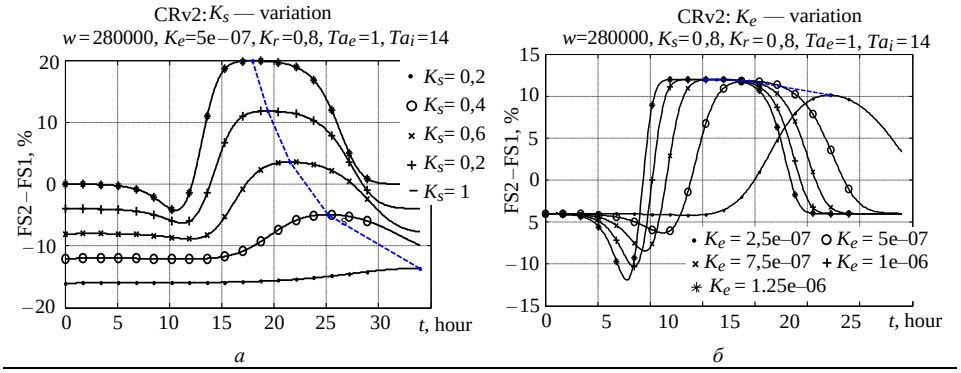
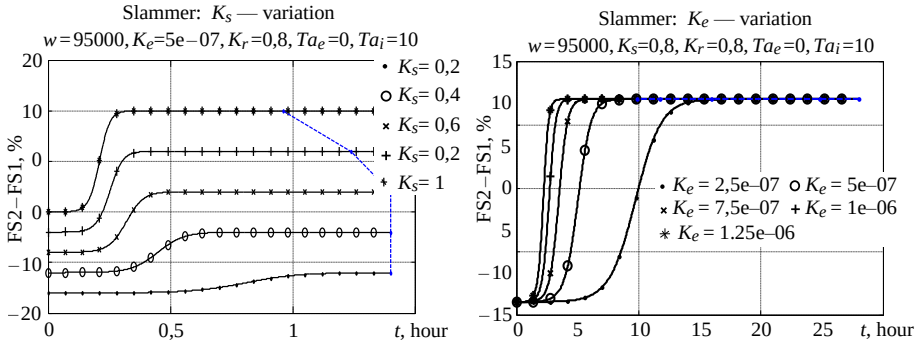
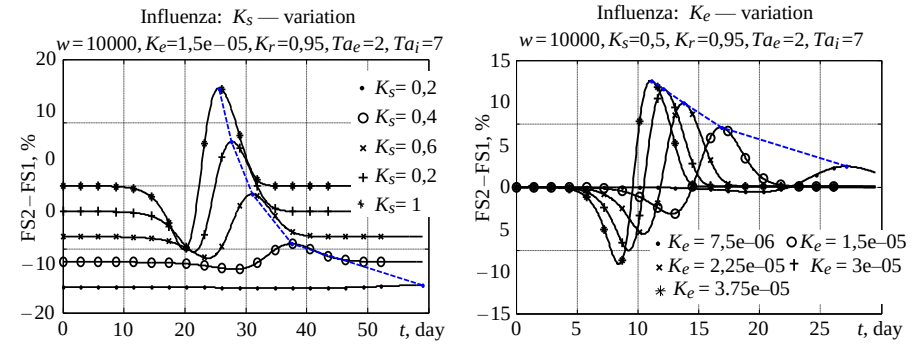


Рис. 6



а *б*

Рис. 7



а *б*

Рис. 8

Результаты исследования зависимости погрешности оценки функциональности ИС ΔFS от параметров K_s, K_e обобщены в табл. 2 (эпидемии ИС) и табл. 3 (эпидемия гриппа).

Таблица 2

Вид эпидемии	Параметр	Этапы							
		До роста		Рост		Лечение		Спад	
		min, %	max, %	min, %	max, %	min, %	max, %	min, %	max, %
CRv1	K_s	– 12	0	– 12	+ 20	– 12	20	– 12	+ 20
	K_e	– 3	– 3	– 22	+ 14	14	14	– 3	+ 14
CRv2	K_s	– 16	0	– 16	+ 20	– 16	+20	– 13	+ 20
	K_e	– 4	– 4	– 12	+ 12	+12	+12	– 4	+ 12
SQL Slammer	K_s	– 16	0	– 16	+ 2	– 16	+ 20	—	—
	K_e	– 4	– 4	– 4	+ 12	+ 12	+ 12	—	—
Всего		– 16	0	– 22	+ 20	– 16	+ 20	– 13	+ 20

Таблица 3

Вид эпидемии	Параметр	Этапы							
		До роста		Рост		Лечение		Спад	
		min, %	max, %	min, %	max, %	min, %	max, %	min, %	max, %
Грипп	K_s	– 16	0	– 16	+16	– 16	+ 16	– 16	+ 16
	K_e	– 10	– 10	– 16	– 2	– 2	– 8	– 10	– 2
Всего		– 6	0	– 16	+ 16	– 16	+ 16	– 16	+ 16

Заключение

1. В работе предложена модель динамики изменения функциональной устойчивости информационных систем в условиях компьютерных эпидемий.

2. Универсальность модели позволила использовать ее также для моделирования медицинских эпидемий.

3. Работоспособность модели проверена на примере моделирования эпидемий компьютерных червей CodeRed CRv1, CRv2, SQL Slammer, а также эпидемии гриппа в Украине.

4. В результате моделирования установлено, что предложенный подход повышает точность прогнозирования функциональности информационных систем в условиях компьютерной эпидемии от – 22 % (случай завышения оценки традиционным методом) до + 20 % (случай занижения оценки традиционным методом) с учетом знака.

5. При прогнозировании функциональности трудовых ресурсов общества предложенный подход к моделированию увеличивает точность прогнозирования функциональности в условиях эпидемии гриппа от 16 % (завышение оценки традиционным методом) до + 16 % (занижение оценки традиционным методом) с учетом знака.

6. Направлениями дальнейших исследований является апробация модели на принципиально новых видах заражений.

О.С. Бичков, Г.П. Дімітров, В.Л. Шевченко, А.В. Шевченко

УДОСКОНАЛЕННЯ МОДЕЛІ КОМП'ЮТЕРНИХ ЕПІДЕМІЙ ШЛЯХОМ ОЦІНЮВАННЯ ФУНКЦІОНАЛЬНОЇ СТІЙКОСТІ ІНФОРМАЦІЙНОЇ СИСТЕМИ

В умовах постійних комп'ютерних атак багато об'єктів інформаційних систем продовжують працювати і після часткової втрати функціональної стійкості. Для протидії інцидентам потрібно прогнозувати динаміку зміни функціональної стійкості інформаційних систем для поліпшення планування ресурсів протидії. Мета статті — вдосконалити існуючі моделі комп'ютерних епідемій шляхом оцінювання функціональної стійкості інформаційної системи. У роботі вдосконалено динамічну VNF-модель комп'ютерної епідемії, яка дозволяє прогнозувати рівень функціональної стійкості інформаційної системи на різних етапах епідемії. Багато моделей комп'ютерних епідемій було отримано шляхом адаптації моделей біологічних епідемій до особливостей комп'ютерних об'єктів. VNF-модель сприяла поліпшенню моделей біологічних епідемій шляхом зворотньої адаптації моделей комп'ютерних епідемій до особливостей біологічних об'єктів. Розглянуто логіку взаємних трансформацій між біологічними і комп'ютерними моделями епідемій. VNF-модель враховує, що покращенню функціональної стійкості, крім незаражених об'єктів, можуть сприяти також об'єкти, інфіковані на різних стадіях зараження, і об'єкти, які вилікувані, але втратили частину своєї функціональної стійкості. Досліджено динамічну залежність похибки оцінки функціональної стійкості від коефіцієнта сприйнятливості до зараження і коефіцієнта передачі зараження. Запропоновану модель апробовано на прикладах реальних епідемій комп'ютерних хробаків CodeRed CRv1, CRv2, SQL Slammer і епідемії грипу в Україні. Запропонований підхід підвищив точність прогнозування функціональної стійкості інформаційних систем в умовах комп'ютерної епідемії до 22 % і збільшив точність прогнозування функціональної стійкості трудових ресурсів суспільства в умовах епідемії грипу до 16 %.

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

A.S. Bychkov, G.P. Dimitrov, V.L. Shevchenko, A.V. Shevchenko

IMPROVING OF COMPUTER EPIDEMICS MODEL BY EVALUATING THE FUNCTIONAL STABILITY OF THE INFORMATION SYSTEM

In conditions of constant computer attacks, many objects of information systems continue to work even after a partial loss of functional stability. To resist incidents, it is necessary to predict the dynamics of changes in the functional stability of information systems to improve counteraction resource planning. The purpose of the article is to improve existing models of computer epidemics by assessing the functional stability of the information system. The work improves the dynamic VNF model of a computer epidemic, which allows predicting the level of functional stability of the information system at various stages of the epidemic. Many models of computer epidemics were obtained by adapting models of bio-

logical epidemics to the characteristics of computer objects. The VNF model made it possible to improve models of biological epidemics by reverse adaptation of computer epidemic models to the characteristics of biological objects. The logic of mutual transformations between biological and computer models of epidemics is considered. The VNF model takes into account that, in addition to uninfected objects, then objects infected at different stages of infection and objects that have been cured but lost some of their functional stability can also contribute to functional stability. We investigated the dynamic dependence of the error in assessing functional stability on the coefficient of susceptibility to infection and the transmission coefficient of infection. The proposed model has been tested on examples of real epidemics of computer worms CodeRed CRv1, CRv2, SQL Slammer and the flu epidemic in Ukraine. The proposed approach has increased the accuracy of forecasting the functional stability of information systems in a computerized epidemic to 22 % and increased the accuracy of forecasting the functional stability of the labor force of a society in an epidemic of influenza to 16 %.

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

1. Шевченко В.Л. Кращі світові практики управління інформаційною безпекою та їх вплив на економічну стабільність держави. *Сучасний захист інформації.* Київ : ДУТ, 2015. № 4. С. 4–9.
2. The global state of information security Survey 2016. Turnaround and transformation in cybersecurity. *Офіційний сайт PricewaterhouseCoopers.* 2016. https://www.pwc.com/gx/en/ issues/cyber-security/information-security-survey.html (accessed 23 March 2017)
3. Petrov P., Dimitrov G., Ivanov S. A comparative study on websecurity technologies used in Irish and Finnish Banks. *18 International MultidisciplinaryScientificGeoconference SGEM 2018: Conference Proceedings*, 2–8 July 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.
4. Машков О.А., Барабаш О.В. Оцінка функціональної стійкості розподілених інформаційно-керуючих систем. *Фізико-математичне моделювання та інформаційні технології.* 2005. Вип. 1. С. 157–163.
5. Cohen F. Computer viruses. PhD thesis. University of Southern California. 1985. — 152 p.
6. 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. doi: 10.1109/RISP.1991.130801.
7. Бычков А.С., Новотна В., Шевченко В.Л., Шевченко А.В. Совершенствование модели компьютерных эпидемий на основе расширения множества возможных состояний объектов информационной системы. *Международный научно-технический журнал «Проблемы управления и информатики»*. 2019. № 6. С. 71–85.
8. Kermack W.O., McKendrick A.G. A contribution to the mathematical theory of epidemics. *Proc. Roy. Soc. Lond. A.* 1927. **115**. С. 700–721. DOI: 10.1007/bf02464423.
9. 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.
10. 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.
11. Климентьев К.Е. Компьютерные вирусы и антивирусы: Взгляд программиста. М. : ДМК Пресс, 2013. 656 с.
12. Stollenwerk N., Jansen V. Population biology and criticality. From Critical Bith-Death Processes to Self-Organized Criticality in mutation pathogen system. London : Imperial College Press. 2011. 224 p. doi: 10.1142/P645.
13. Zhang Ch. Global behavior of a computer virus propagation model on multilayer networks. *Hindawi. Security and Communication Networks.* Art.ID 2153195. 2018. **2018**. P. 1–9. https://doi.org/10.1155/2018/2153195.
14. Zhang Z., Song L. Dynamics of a computer virus propagation model with delays and graded infection rate. *Hindawi. Advances in Mathematical Physics.* 2017. Article ID 4514935. P. 1–13. https://doi.org/10.1155/2017/4514935.
15. Umbreen Fatima, Mubasher Ali, Nauman Ahmed, Muhammad Rafiq Malik. 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. Leveille J. Epidemic spreading in technological networks. 2002. 100 p. www.hpl.hp.-com/techreports /2002/HPL-2002-287.pdf (accessed 23 March 2017).
17. Shevchenko A., Shcheblanin J., Shevchenko V. The epidemiological approach to prognosis and management of information incidents. *Системи обробки інформації.* 2017. № 4 (29). С. 145–150. http://www.hups.mil.gov.ua/periodic-app/journal/nitps/2017/4
18. 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

Получено 20.06.2019
После доработки 13.08.2019