УДК 004.94

Типизация сценариев управления защитой сложных технических объектов при неопределенных начальных условиях на основе моделей искусственных иммунных систем

Typing of protection management scenario of complex technical objects under uncertain initial conditions on the basis of models of artificial immune systems

Доронина / Doronina Yu.
Юлия Валентиновна
(JVDoronina@sevsu.ru)
доктор технических наук, доцент.
ФГАОУ ВО «Севастопольский государственный университет» (СевГУ),
профессор кафедры информационных технологий и компьютерных систем.
г. Севастополь

Моисеев / Moiseev D.
Дмитрий Владимирович
(DVMoiseev@sevsu.ru)
доктор технических наук, доцент.
СевГУ, профессор кафедры информационных технологий и компьютерных систем.
г. Севастополь

Скатков / Skatkov A.
Александр Владимирович
(AVSkatkov@sevsu.ru)
доктор технических наук, профессор.
СевГУ,
профессор кафедры информационных технологий и компьютерных систем.
г. Севастополь

Ключевые слова: искусственные иммунные системы – artificial immune systems; атаки вирусного типа – virus-type attacks; сложный технический объект – complex technical object; неопределенность начальных условий – uncertainty of initial conditions; траектория процесса – process trajectory; сценарий защиты – protection scenario.

Предложен подход к типизации сценариев управления защитой сложных технических объектов при атаках вирусного типа на основе модели искусственных иммунных систем. В предположениях о соответствии параметров модели искусственных иммунных систем параметрам сложных технических систем проведены модельные эксперименты, отражающие процесс функционирования антивирусной защиты сложного технического объекта. На основе предложенного конструктивного подхода получена основа оперативного инструмента принятия решений по параметрической и функциональной настройке систем защиты сложных технических объектов на долгосрочную и краткосрочную перспективы.

An approach to the typification of scenarios for managing the protection of complex technical objects in virus-type attacks based on a model of artificial immune systems is proposed. Under the assumption that the parameters of the model of artificial immune systems correspond to the parameters of complex technical systems, model experiments were carried out reflecting the process of functioning of the antivirus protection of a complex technical object. Based on the proposed constructive approach, the basis of an operational decision-making tool for parametric and functional configuration of protection systems for complex technical objects for the long and short term is obtained.

Введение

Управление защитой сложных технических объектов (СТО) от атак вирусного типа представляет собой важную и актуальную задачу в связи с интенсификацией угроз подобного типа. Под управлением защитой СТО от вирусных атак понимается решение задачи по выбору:

– глубины (степени детализации анализа проблемы: внешние, внутренние проблемы),

– частости (интенсивности мер по защите),

– мощности (объема применения базы антивирусных средств).

Для СТО, подвергающихся атакам вирусного типа, рост исходных данных и время реакции системы защиты на атаку играет важную роль, в связи с чем целесообразным представляется применение сценарного подхода, основанного на определении типизированных сценариев реакции системы защиты.

Построение системы защиты СТО тесно связано с моделированием вирусной атаки, что предложено сделать на основе модели искусственных иммунных систем (ИИС).

Таким образом, под сценарием будем понимать в общем случае последовательность шагов (дерево) принятия решений по формированию требуемого уровня иммунитета системы относительно уровня вирусной атаки для выбранных состояний СТО.

Решения системы обыкновенных дифференциальных уравнений (ОДУ), описывающей динамику искусственных иммунных систем, в значительной степени определяются начальными условиями, которые повторить в большинстве случаев не представляется возможным в связи со сложностью объекта ИИС.

В этой связи актуален выбор управляющих решений при неопределенных начальных условиях дифференциальных моделей ИИС. Особенностью изучения процессов защиты сложных объектов с учетом общих закономерностей функционирования ИИС является возможность сопоставления технических устройств живым организмам в свете наличия операционной возможности нейтрализации вирусной программы посредством антивирусного иммунитета [7–11, 15–17].

Предположение о том, что начальные условия дифференциальных моделей ИИС неопределенные, позволило реализовать моделирование процессов вирусного заражения, приближенных к реальным, при управлении их защитой.

Исследованию подходов к управлению защитой сложных технических объектов от вирусных атак посвящено немало современных работ [1–5]. Моделирование состояния таких систем на основе искусственных иммунных систем предложено авторами в работах [4–6].

Важным представляется исследование влияния случайных отклонений при установке заданных (номинальных) значений начальных условий на реальном объекте; случайные воздействия внешней среды на объект, изменяющие реальные выходные характеристики по отношению к расчетным; влияние изменяющихся, как правило, неслучайным, но заранее неизвестным образом, условий функционирования объекта, например таких, как температура, влажность, вибрации, уровень радиации и т. д. [8].

В отличие от типичных признаков неопределенности начальных условий авторы предлагают исследовать атипичную неопределенность эллипсного типа, когда точки решения находятся внутри условных эллипсов вследствие влияния начальных условий на решения ОДУ.

Таким образом, предложенный подход к управлению защитой СТО на основе модели ИИС с неопределенными начальными условиями ОДУ позволил на основе результатов моделирования сформулировать типизацию принципов такого управления в рамках сценарного подхода и обоснованно планировать операции и состав мероприятий по антивирусной защите, что и составляет содержание статьи.

Моделирование иммунного ответа ИИС с неопределенными начальными условиями на основе эллипсов рассеяния

Математическая модель реакции сложного технического объекта на вирусную атаку в соответствии с [3, 10, 13] строится на основе соотношений баланса для каждой из зависимых переменных в предположении, что СТО описывается однородным замкнутым объемом, в котором все компоненты процесса равномерно перемешаны.

Изменение числа и сложности антивирусных алгоритмов (количество операций), участвующих в процессе иммунного ответа на отрезке времени $[t_0, T]$, где $t_0 = 0$ – момент инфицирования СТО, в отличие от известной схемы решения в виде нелинейных дифференциальных уравнений с запаздывающим аргументом, записанных в нормальной форме Коши, с учетом интерпретации базовых параметров в ИИС, с учетом фазовых ограничений $V(t) \geq 0.0$, $F(t) \geq 0.0$, $C(t) \geq 0.0$, запишется в виде

$$\frac{dV}{dt} = \beta V - \gamma FV\ ,\ \frac{dF}{dt} = \rho C - \eta\gamma FV - \mu_f F \qquad (1)$$

с начальными условиями:

$$V(0) = V^0,\ F(0) = F^0,\ C(0) = C^0 \qquad (2)$$

и фазовыми ограничениями: $V(t) \geq 0.0$, $F(t) \geq 0.0$, $C(t) \geq 0.0$, где $\beta > 0$ — скорость (темп) размножения антигенов; $\gamma > 0$ – коэффициент, учитывающий вероятность нахождения вредоносного кода; $\rho > 0$ – скорость реализации операций антивирусной программы; $\mu_f > 0$ – величина, обратная продолжительности активности алгоритма антивируса; $\eta > 0$ – количество функций, необходимое для нейтрализации одного вируса; $V^* = V^*(t)$ – относительное количество вирусов для рассматриваемого ресурса; $C^* = C^*(t)$ – относительный объём антивирусной базы (объём памяти); $F^* = F^*(t)$ – относительная сложность антивирусных алгоритмов (количество операций).

Параметры в (1) могут быть интерпретированы, например, для процессоров:

$V^*_{\text{Пр}}$ – относительное количество вычислительных операций во вредоносном коде;

$F^*_{\text{Пр}}$ – относительное количество вычислительных операций в антивирусном алгоритме, необходимых для нейтрализации вирусной атаки;

$C^*_{\text{Пр}}$ – относительное количество вирусных сигнатур в антивирусных базах;

– при анализе запоминающих компонент СТО, интерпретация параметров ИИС:

$V^*_{\text{Пм}}$ – относительный объём вредоносного кода;

$F^*_{\text{Пм}}$ – относительный объём антивирусного кода, необходимый для нейтрализации вирусной атаки;

$C^*_{\text{Пм}}$ – относительный объём антивирусных баз [1].

В зависимости от начальных условий изменяется иммунный ответ ИИС на внешнюю атаку, причём основным критерием является относительное начальное количество $F(0)$. Считаем, что в СТО не происходит полного поражения атакуемого ресурса, поскольку ещё на предварительных стадиях видно ухудшение характеристик работы системы, то становится очевидна атака и происходит автоматическая остановка вычислительного процесса. В связи с этим целесообразно исследование статистической устойчивости системы ОДУ в модели иммунного ответа ИИС относительно неопределенных начальных условий.

Рассмотрим уравнения системы (1), отражающие в ИИС оценки относительной сложности антивирусных алгоритмов (количество операций) и относительное количество вирусов для рассматриваемого сценария защиты.

На рис. 1 приведены результаты решения ОДУ по *F, V* и моделирования изменчивости точек фазового пространства координат F и V при начальных условиях (2), образованных упорядоченными выборками $V(0) = 0.1,...,0.8$, $F(0) = 0.4,...,1.0$, $C(0) = \text{const}$ для моментов условного времени $t_1 = 1..14$.

Относительное количество операций в вирусных алгоритмах V начинает значительно уменьшаться из-за наличия антивирусных операций F, поражаемый объект испытывает на себе поражающее воздействие вирусов и снижение объема оперативной памяти (замедление скорости обработки) от работы антивирусных операций, рис. 1. После превышения в относительном объёме антивирусных операций над вирусными, их количество перестаёт увеличиваться и начинает постепенно уменьшаться ($t = 2.0$). Относительное количество операций антивируса также постоянно уменьшается. Начиная с $t = 3.0$ начинается регенерация поражаемого объекта.

На рис. 2 приведены результаты изменчивости группировки точек фазового пространства координат F и V в некотором диапазоне значений начальных условий, имитирующем варианты начальных состояний СТО: $V(0) = 0.1,...,0.8$, $F(0) = 0.4,...,1.0$.

Анализ динамики изменчивости группировки точек решений ОДУ – модель искусственной иммунной системы (отражающей уровни антивирусной защиты системы), рис. 2, свидетельствует о регуляризации процессов в ИИС с течением времени при динамичности начальных условий. Используем понятия диаметров эллипсов рассеяния и угловых коэффициентов (коэффициентов k в уравнении прямой $y = kx + b$ на координатной плоскости, соответствующей оси группировки точек), рис. 3.

На основании приведенных результатов моделирования, рис. 2 и схем анализа группировки точек в эллипсах рассеяния, рис. 3, выделим три основных типа конфигурации группировки точек:

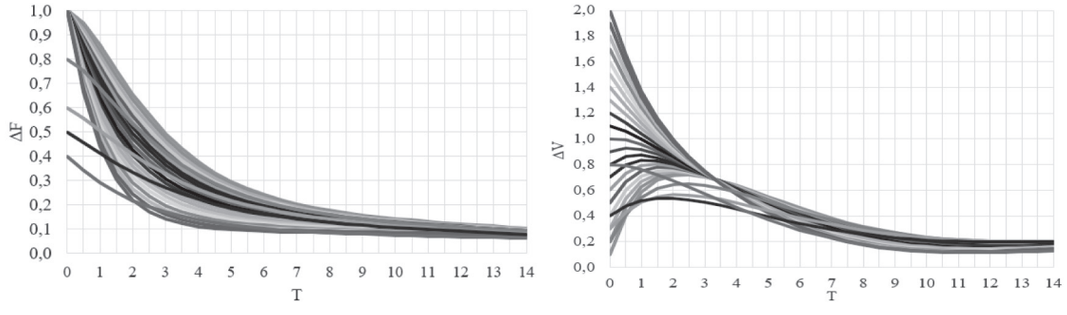
– угловой коэффициент $k < 0$ (угол $\lambda > 90°$) – (А зона) – рис. 2, a), b), c), d);

– угловой коэффициент $k > 0$ (угол $\lambda < 90°$) – (В зона) – рис. 2, e), f), g);

– угол λ не существует или стремится к нулю, так как группа стянута в точку – (С зона) – рис. 2, h).

Для углового коэффициента $k > 0$, угол $\lambda = 90°$ или $\lambda < 90°$ (В зона) и $\lambda = \text{arctg}(k)$; при $k < 0$, (А зона), $\lambda = \pi - \text{arctg}|k|$.

На рис. 4 приведены результаты оценок соответствия разброса группировки точек и углов наклона



a *b*

Рис. 1. Результаты моделирования размножения вирусов и иммунного ответа ИИС в диапазоне значений начальных условий: a – изменение числа операций в антивирусных алгоритмах ΔF; b – изменение вирусных алгоритмов ΔV в диапазоне t=1.0...14.0

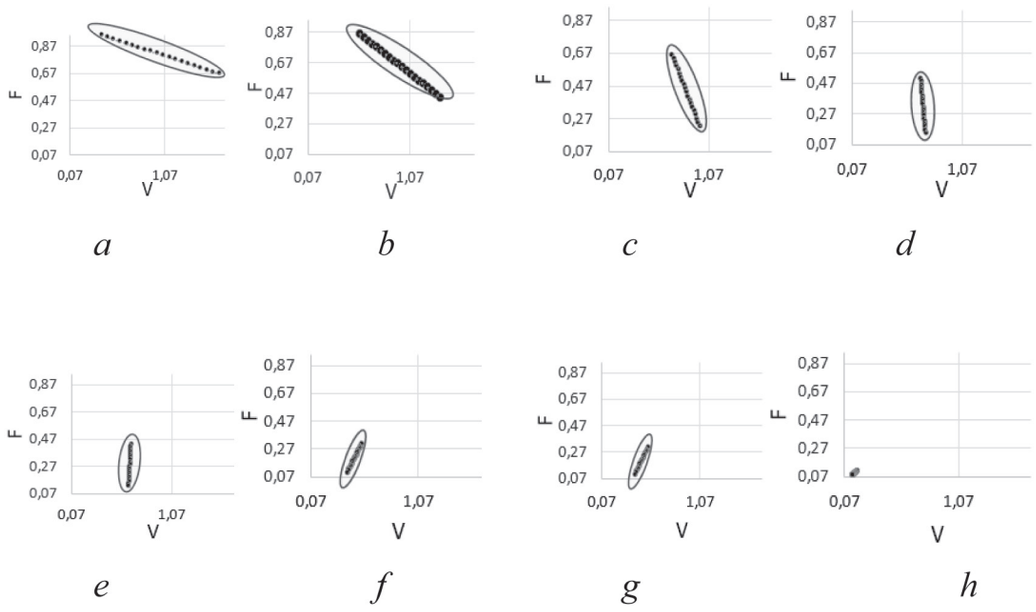


Рис. 2. Результаты моделирования изменчивости группировки точек фазового пространства координат F и V в диапазоне значений начальных условий:
$a - t_1 = 0.5$; $b - t_2 = 1.0$; $c - t_3 = 2.0$; $d - t_4 = 3.0$; $e - t_5 = 3.5$; $f - t_6 = 4.0$;
$g - t_7 = 5.0$; $h - t_8 = 14.0$

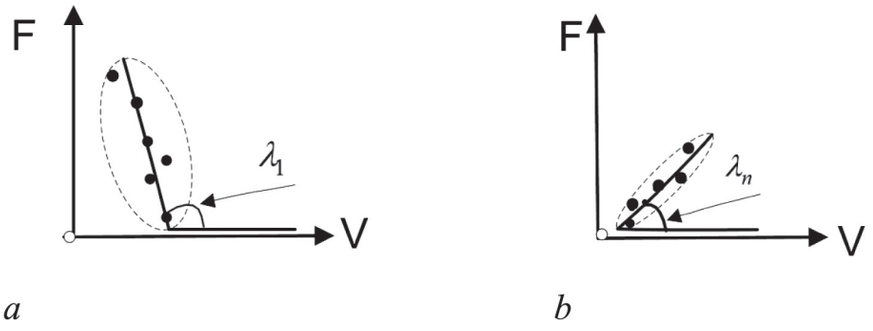


Рис. 3. Схемы анализа группировки точек в эллипсах рассеяния по результатам моделирования размножения вирусов и иммунного ответа: a – угол $\lambda > 90°$ *; b – угол* $\lambda < 90°$

к оси абсцисс в зависимости от условных единиц времени $t = 0.5..14.0$. Угол наклона рассчитывался на основе углового коэффициента, полученного путем аппроксимирования группировок точек, рис. 2.

При достаточно общей постановке задачи речь идет о типизации сценариев управления защитой СТО по траекториям иммунного ответа ИИС относительно начальных условий ОДУ.

Сценарный подход к анализу вида решений дифференциальных уравнений в модели иммунного ответа ИИС с неопределенными начальными условиями

Под сценарием понимается дерево принятия решений по формированию требуемого уровня иммунитета относительно уровня вирусной атаки. Для формирования сценария управления необходимо сопоставить состояниям СТО, определяемым декартовым произведением F и V, соответствующие управления параметрами ИИС, приводящие систему в требуемое состояние из множества: $S = \{S^{\mathrm{I}}, S^{\mathrm{II}}, S^{\mathrm{III}}\}$, где элементы множества – классы состояний с достаточным, номинальным уровнем и недостаточным уровнем иммунитета соответственно.

При детерминированных условиях эксперимента, рис. 1, естественный переход ИИС в состояние S^{II} осуществляется при $3 < t < 3.5$, что соответствует $\lambda = 90°$, (рис. 2, d),e)) и $F^0 > 0.49$, $V^0 > 0.7$; в S^{III} осуществляется при $10 \le t \le 14$, что соответствует острому углу λ, (рис. 2, h)) и $F^0 > 0.14$, $V^0 > 0.23$ и при дальнейшем увеличении временного интервала множество решений стягивается в точку.

Рассмотрим факторы управления $U_{j,i,k}$ защитой СТО:

$$U_{j,i,k}(\beta_i, \gamma_i, \tau_j, f_k^0),\ j \in J,\ k \in K,\ i \in I \qquad (3)$$

где f_k^0 – начальный уровень иммунитета (антивирусной защиты); $\beta_i > 0$ – скорость (темп) размножения антигенов при заданном f_k^0 (соответствует показателю интенсивности защиты);

$\gamma_i > 0$ – коэффициент, учитывающий вероятность встречи вирусов с антителами и силу их взаимодействия при f_k^0 (соответствует мощности защиты СТО); J – множество индексов различных управлений; I – множество индексов, соответствующих различным параметрам ИИС; K – множество индексов, характеризующих состояние СТО (например, при f_k^0 и γ_i может достигаться β_i); τ_j – момент времени обнаружения атаки; L – множество индексов, определяющих моменты времени.

Требуется найти такое управление $U_{j,i,k}$ при некоторых $f_k \cdot v_k$, начальном уровне иммунитета f_k^0, чтобы обеспечить переход СТО из S^{III} (состояния с недостаточным иммунитетом) в состояния с достаточным или номинальным иммунитетом S^{I} или S^{II} (в зависимости от цели управления).

Определим состояние СТО в начальный момент времени при фиксированных параметрах β_i, γ_i:

$$\psi_0(t_0) | \beta_i, \gamma_i,$$

где $\psi_0(t_0)$ – состояние СТО из множества различимых состояний $\psi_k = \{\psi_1, ..., \psi_K\}$ в момент времени t_0; обозначим $D_k = f_k \cdot v_k$ – значение контролируемой характеристики k-го состояния СТО.

Всюду далее символом "$\rightarrow$" будем обозначать отображение, осуществляемое при смене состояний СТО при начальном уровне иммунитета f_k^0 или при изменении параметров β_i, γ_i с целью дальнейшей

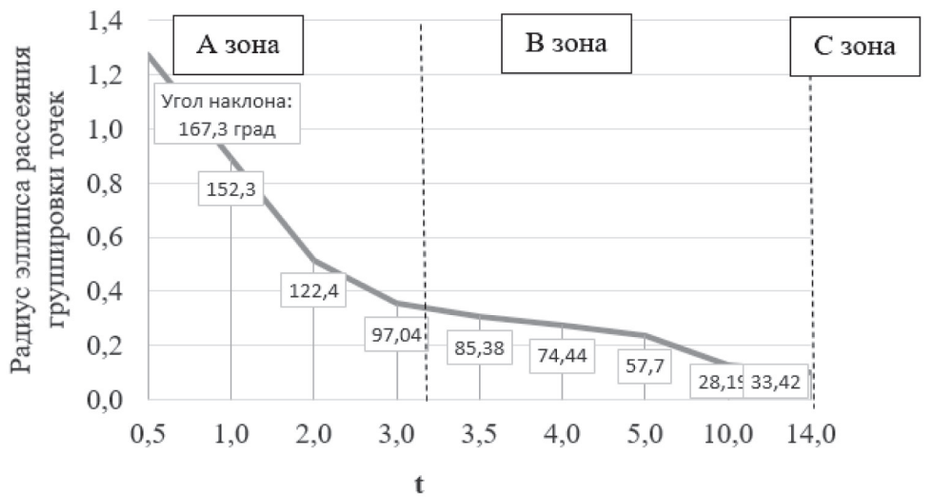


Рис. 4. Оценивание разброса группировки точек и углов наклона к оси абсцисс в зависимости от времени t с типизаций зон

возможной классификации реакций регулятора управления ресурсами защиты.

При $\left|f_k^i(t)-f_{k+1}^i(t)\right| \le f_{\min}^i$, $\left|v_h^i(t)-v_{h+1}^i(t)\right| \ge v_{\max}^i$, где $f_{\min}^i$ и $v_{\max}^i$ – критические значения f_k^i и v_k^i, смена состояния СТО имеет вид: $(\psi_0(t_0)|\beta_j,\gamma_j) \to (\psi_1(t_1)|\beta_j,\gamma_j)$, то есть критическое изменение значений показателей СТО f_k^i и v_k^i, за время Δt изменяет состояние $\psi_k(t_i)$; $\Delta t = t_1 - t_{l-1}$ – промежуток между двумя соседними моментами времени; t_l – l-й момент времени измерения характеристик, $t_l \in [0;L]$.

Представим матрицей соответствие точек фазового пространства координат F и V, в которой $\psi_k(t_i)$ определяет некоторый требуемый уровень состояния атакуемой вирусом системы в момент времени t_i.

$$\begin{array}{c} \\ F_0 \\ \dots \\ F_m \end{array} \begin{array}{c} \begin{array}{ccc} V_0 & \dots & V_n \end{array} \\ \begin{pmatrix} \psi_0(t_0) & \dots & \omega_2 : \psi_0(t_k) \\ \dots & \omega_1 : \psi_1(t_1) & \dots \\ \omega_d : \psi_k(t_l) & \dots & \omega_m : \psi_k(t_d) \end{pmatrix} \end{array} \quad (4)$$

В рамках некоторого интервала времени T на основе изменения D_j формируются траектории $\omega_i \in \{\omega_1,\omega_2,...,\omega_m,\omega_d\}, m,d \in \Theta$, где Θ – множество допустимых траекторий, на которых определяются состояния СТО $\psi_k(t_i)$, рис. 5.

Для трех траекторий, изображенных на рис. 5, и трех наборов начальных условий: f_0^1, v_0^1; f_0^2, v_0^2; f_0^3, v_0^3, имеем:

$$\begin{aligned}
&\omega_1 : (\psi_0^{\mathrm{I}}(t_0)|[\beta_j,\gamma_j;f_0^1,v_0^1]) \to (\psi_1^{\mathrm{II}}(t_1)|[\beta_j,\gamma_j;f_1^1,v_1^1]) \to \\
&\to (\psi_2^{\mathrm{II}}(t_2)|[\beta_j,\gamma_j;f_1^1,v_2^1]) \to (\psi_3^{\mathrm{III}}(t_3)|[\beta_j,\gamma_j;f_2^1,v_2^1]); \\
&\omega_2 : (\psi_0^{\mathrm{I}}(t_0)|[\beta_j,\gamma_j;f_0^2,v_0^2]) \to (\psi_1^{\mathrm{II}}(t_1)|[\beta_j,\gamma_j;f_1^2,v_0^2]) \to \\
&\to (\psi_2^{\mathrm{III}}(t_2)|[\beta_j,\gamma_j;f_2^2,v_0^2]) \to (\psi_3^{\mathrm{III}}(t_3)|[\beta_j,\gamma_j;f_2^2,v_1^2]); \\
&\omega_3 : (\psi_0^{\mathrm{I}}(t_0)|[\beta_j,\gamma_j;f_0^3,v_0^3]) \to (\psi_1^{\mathrm{I}}(t_1)|[\beta_j,\gamma_j;f_0^3,v_1^3]) \to \\
&\to (\psi_2^{\mathrm{II}}(t_2)|[\beta_j,\gamma_j;f_1^3,v_2^3]) \to (\psi_3^{\mathrm{III}}(t_3)|[\beta_j,\gamma_j;f_2^3,v_2^3]);
\end{aligned} \quad (5)$$

Изменение начальных условий ведет к изменению траектории ω_i, а число выделенных зон для типизации разброса точек может быть выбрано, исходя из требований ЛПР. В данном исследовании использованы три зоны, рис. 2, сформированных относительно угла наклона направляющей в группировках точек.

При наличии управления $U_{j,i,k}$ формальное представление модифицируемой траектории с учетом выражений (5) примет вид:

$$\begin{aligned}
&\omega_i^{\mathrm{I}\to\mathrm{II}} : (\psi_0^{\mathrm{I}}(t_0)|[\beta_0,\gamma_0;f_0^i,v_0^i]) \xrightarrow{f_k^i \le f_{\min(I)}^i, v_h^i \ge v_{\max(I)}^i} \\
&(\psi_1^{\mathrm{II}}(t_l)|[\beta_p,\gamma_p;f_1^i,v_1^i]); \\
&\omega_i^{\mathrm{II}\to\mathrm{III}} : (\psi_1^{\mathrm{II}}(t_1)|[\beta_p,\gamma_p;f_1^i,v_1^i]) \xrightarrow{f_k^i \le f_{\min(II)}^i, v_h^i \ge v_{\max(II)}^i} \\
&(\psi_3^{\mathrm{III}}(t_3)|[\beta_q,\gamma_q;f_k^i,v_h^i]); \\
&i=\overline{1,I};\ k=\overline{1,K};\ h=\overline{1,H};\ \beta_0,\gamma_0,\beta_p,\gamma_p,\beta_q,\gamma_q \in \{B,\Gamma\},
\end{aligned} \quad (6)$$

где I – число возможных (допустимых) траекторий; K – число возможных операций в антивирусных алгоритмах; H – число возможных операций в вирусных алгоритмах; $\{B,\Gamma\}$ – множество управляющих реакций ИИС, "$\xrightarrow{f_k^i \le f_{\min(I)}^i, v_h^i \ge v_{\max(I)}^i}$" – отображение, осуществляемое при смене состояний СТО и выполнении условий перехода $f_k^i < f_{\min(I)}^i$, $v_h^i \le v_{\max(I)}^i$, где $f_{\min(I)}^i$ и $v_{\max(I)}^i$ – критические значения параметров f_k^i и v_h^i.

Таким образом, с учетом (6) в табл. 1 определены следующие возможные основные типы сценариев управления защитой СТО на основе модели ИИС. Использованы виды требуемых управлений: стабилизация состояния, стабилизация и накопление иммунитета системой защиты, стабилизация и удержание состояния СТО.

Типизация сценариев управления защитой сложных технических объектов при неопределенных начальных условиях

В связи с тем, что защита СТО от вирусных атак представляет собой процесс, критичный по отно-

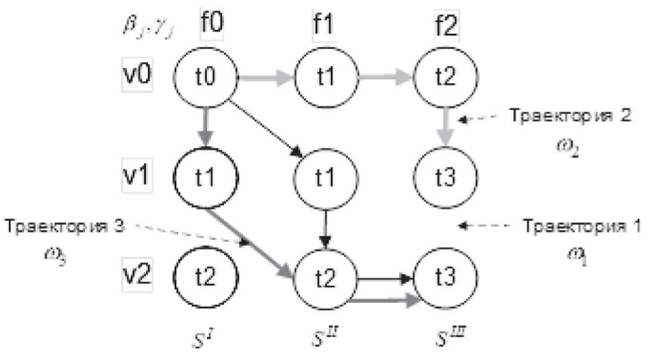
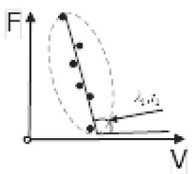
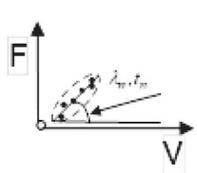


Рис. 5. Граф траекторий состояний атакуемой системы относительно начальных условий f_0, v_0

Таблица 1

Основные типы сценариев управления защитой сложного технического объекта на основе модели искусственных иммунных систем

Элемент сценария управления защитой СТО (название столбца 1 на английском языке)	Вид зоны разброса точек и углов наклона центров группировок к оси абсцисс в зависимости от времени *t* (название столбца 2 на английском языке)	Формальное представление сценария на основе представления траектории (название столбца 3 на английском языке)	Вид и содержание требуемого управления
(1) с одним из условий	A: угловой коэффициент $k < 0$ (угол λ тупой) 	$\omega_i^{\mathrm{I}\to\mathrm{II}} : (\psi_0^{\mathrm{I}}(t_0) \mid [\beta_0, \gamma_0; f_0^i, v_0^i]) \to$ $\to (\psi_1^{\mathrm{II}}(t_l) \mid [\beta_p, \gamma_p; f_1^i, v_1^i]);$ Условия: $f_k^i < f_{\min(\mathrm{I})}^i \vee v_h^i \geq v_{\max(\mathrm{I})}^i$	Стабилизация: $\beta_p, \gamma_p : f_{k+1}^i = f_k^i + \Delta f^i$
(1) с двумя условиями		Условия: $f_k^i < f_{\min(\mathrm{I})}^i \wedge v_h^i \geq v_{\max(\mathrm{I})}^i$	$\beta_p, \gamma_p : f_{k+1}^i = f_k^i + \Delta f^i$ $v_{h+1}^i = v_h^i - \Delta\tilde{v}^i$
(2) с одним из условий	B: угловой коэффициент $k > 0$ (угол λ острый) 	$\omega_i^{\mathrm{II}\to\mathrm{III}} : (\psi_1^{\mathrm{II}}(t_1) \mid [\beta_p, \gamma_p; f_1^i, v_1^i]) \to$ $\to (\psi_3^{\mathrm{III}}(t_3) \mid [\beta_q, \gamma_q; f_k^i, v_h^i]);$ Условия: $f_k^i < f_{\min(\mathrm{II})}^i \vee v_h^i \geq v_{\max(\mathrm{II})}^i$	Стабилизация и накопление иммунитета системой защиты: $\beta_q, \gamma_q : f_{k+1}^i = f_k^i + \Delta f^i$ $f_{k+1}^{i+1} = f_k^i + \Delta f$
(2) с двумя условиями		Условия: $f_k^i < f_{\min(\mathrm{II})}^i \wedge v_h^i \geq v_{\max(\mathrm{II})}^i$	$\beta_q, \tilde{\gamma}_q : f_{k+1}^i = f_k^i + \Delta f^i$ $v_{h+1}^i = v_h^i - \Delta\tilde{v}^i$
(4)	C: угловой коэффициент $k > 0$ (угол λ острый) и длина группировки точек $1 \leq 1^*$ (условие стягивания в точку)	$\omega_i^{\mathrm{II}\to\mathrm{III}} : (\psi_1^{\mathrm{II}}(t_1) \mid [\beta_p, \gamma_p; f_1^i, v_1^i]) \to$ $\to (\psi_3^{\mathrm{III}}(t_n) \mid [\beta_q, \gamma_q; f_k^i, v_h^i]);$ Условия: $f_k^i \leq f_{\min(\mathrm{III})}^i \wedge v_h^i \geq v_{\max(\mathrm{III})}^i \wedge$ $\wedge\, l_g^i \leq l_{\max(\mathrm{III})}^i$	Стабилизация и удержание состояния СТО: $\beta_q, \gamma_q : f_{k+1}^i = f_k^i + \Delta f^i$

шению к ресурсу времени, требуются меры повышения оперативности реакции системы защиты. В этой связи формирование типизированных сценариев может быть положено в основу системы поддержки принятия решений по повышению оперативности системы защиты СТО.

С учетом обозначенных в таблице 1 этапов авторами предложены четыре типовых сценария защиты КИО:

– сценарий 1: стабилизация состояния СТО при неопределенности содержания вирусной атаки (имеется неопределенность операций и сигнатур вирусов):

$$\omega_i^{\mathrm{I}\to\mathrm{II}} : (\psi_0^{\mathrm{I}}(t_0)\big|[\beta_0,\gamma_0;f_0^i,v_0^i]) \to (\psi_1^{\mathrm{II}}(t_l)\big|[\beta_p,\gamma_p;f_1^i,v_1^i]);$$

при условиях:

$$f_k^i \le f_{\min(\mathrm{I})}^i [\vee v_h^i \ge v_{\max(I)}^i],$$

с управлением вида:

$$\beta_p,\gamma_p : f_{k+1}^i = f_k^i + \Delta f^i,$$

где Δf^i – некоторый ресурс (накопленный иммунитет) операций антивирусной программы на данной траектории процесса ИИС;

– сценарий 2: стабилизация состояния СТО и наращивание ресурса (накопление иммунитета) при известном содержании вирусной атаки (операции и сигнатуры вирусной программы известны):

$$\omega_i^{\mathrm{II}\to\mathrm{III}} : (\psi_1^{\mathrm{II}}(t_1)\big|[\beta_p,\gamma_p;f_1^i,v_1^i]) \to (\psi_3^{\mathrm{III}}(t_3)\big|[\beta_q,\gamma_q;f_k^i,v_h^i]);$$

при условиях:

$$f_k^i \le f_{\min(\mathrm{II})}^i \vee v_h^i \ge v_{\max(\mathrm{II})}^i,$$

с управлением вида:

$$\beta_p,\gamma_p : f_{k+1}^i = f_k^i + \Delta f^i;\ f_{k+1}^{i+1} = f_k^i + \Delta f;\ v_{h+1}^i = v_h^i - \Delta\tilde{v}^i,$$

где Δf – типовой ресурс операций антивирусной программы; f_{k+1}^{i+1} – ресурс операций антивирусной программы при смене траектории процесса ИИС; $\Delta\tilde{v}^i$ – определенное число операций вирусной программы на текущей траектории процесса ИИС;

– сценарий 3: стабилизация и удержание состояния СТО при определенности содержания вирусной атаки:

$$\omega_i^{\mathrm{II}\to\mathrm{III}} : (\psi_1^{\mathrm{II}}(t_1)\big|[\beta_p,\gamma_p;f_1^i,v_1^i]) \to (\psi_3^{\mathrm{III}}(t_n)\big|[\beta_q,\gamma_q;f_k^i,v_h^i]);$$

Рис. 6. Алгоритмизированная схема системы управления защитой сложных технических объектов на основе типизированного сценарного подхода

при условиях:

$$f_k^i \le f_{\min(\text{III})}^i \vee v_h^i \ge v_{\max(\text{III})}^i \wedge l_g^i \le l_{\max(\text{III})}^i,$$

с управлением вида:

$$\beta_p, \gamma_p : f_{k+1}^i = f_k^i + \Delta f^i.$$

На рис. 6 приведен обобщенный вид алгоритмизированной схемы системы управления защитой СТО на основе типизированного сценарного подхода.

Выводы

Предлагаемый в статье подход к управлению защитой сложных технических объектов основан на исследовании влияния неопределенности начальных условий ОДУ на результаты моделирования в ИИС и формировании на этой основе типизированных сценариев защиты, что позволит реализовать поддержку принятия решений по повышению оперативности защиты от вирусных атак и формирование соответствующих управлений.

На основе предложенных сценариев могут быть сформулированы и другие, в которых последовательность типовых состояний ИИС будет целесообразна для получения определенных эффектов в случаях, например, полиморфных сигнатур вирусных алгоритмов, либо для достижения результатов при заданных типах защиты СТО.

Одним из важных результатов исследования является сам принцип типизации сценариев защиты на основе анализа вида группировок точек, отражающих результаты моделирования иммунного ответа (уровня антивирусной защиты системы) как решений системы ОДУ на основе диаметров рассеяния этих точек и угла наклона аппроксимирующей прямой к оси абсцисс.

На основе предложенного конструктивного подхода получена основа оперативного инструмента принятия решений по параметрической настройке системы защиты сложных технических объектов на долгосрочную и краткосрочную перспективы.

Литература

1. Potential threat vectors to 5g infrastructure / CISA's newest report identiies. – 2021. – URL: https://www.cisa.gov/sites/default/files/publications/potential-threat-vectors-5G-infrastructure_508_v2_0%20%281%29.pdf (дата обращения 14.11.2022).

2. Адаптивное обнаружение уязвимостей интерфейсов беспилотных транспортных средств / А.В. Скатков, А.А. Брюховецкий, Ю.В. Доронина [и др.]. – Симферополь : Издательство Типография «Ариал», 2020. – 352 с.

3. Структурный синтез каналов информационных обменов для беспилотных транспортных средств / А.В. Скатков, Д.В. Моисеев, А.А. Брюховецкий [и др.]. – Симферополь : Издательство Типография «Ариал», 2020. – 320 с.

4. Secure communication channel architecture for Software Defined Mobile Networks / M. Liyanage, A. Braeken, A.D. Jurcut [et al.] // Computer Networks. – 2017. – Vol. 114. – P. 32–50.

5. Secure Machine-Type Communications toward LTE Heterogeneous Networks / C. Zhao, L. Huang, Y. Zhao, X. Du // IEEE Wireless Communications. – 2017. – Vol. 24, No. 1. – P. 82–87.

6. A First Look at Commercial 5G Performance on Smartphones / A. Narayanan, E. Ramadan [et al.] // Proceedings of The Web Conference 2020 (WWW'20) (April 20–24, 2020, Taipei, Taiwan). – 2020. – P. 894–905.

7. A Misbehavior Authority System for Sybil Attack Detection in C-ITS / J. Kamel, F. Haidar, I. Ben Jemaa [et al.] // The IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference – IEEE UEMCON 2019 (New York, October, 2019). – P. 1117–1123.

8. Van der Heijden, R. W. VeReMi: A Dataset for Comparable Evaluation of Misbehavior Detection in VANETs / R.W. van der Heijden, T. Lukaseder, F. Kargl // International Conference on Security and Privacy in Communication Systems. – 2018. – P. 318–337.

9. Luxembourg sumo traffic (lust) scenario: Traffic demand evaluation / L. Codeca, R. Frank, S. Faye, T. Engel // IEEE Intelligent Transportation Systems Magazine. – 2017. – Vol. 9, No. 2. – P. 52–63.

10. Скатков, А. В. Коллаборационные стратегии обнаружения уязвимостей интерфейсов информационно-измерительных сетей ПТС при технологиях 5G / А.В. Скатков, А.А. Брюховецкий // Системы контроля окружающей среды. – 2022. – № 49 (3). – С. 84–97.

11. Скатков, А. В. Модели коллабораций обнаружения уязвимостей интерфейсов беспилотных транспортных средств в условиях противодействия на основе стандарта 5G / А.В. Скатков, А.А. Брюховецкий, Д.В. Моисеев // Информация и Космос. – 2022. – № 4. – С. 58–65.

12. Modeling of monitoring processes of structurally heterogeneous technological objects / A. Skatkov, V. Shevchenko, D. Voronin, D. Moiseev // MATEC Web of Conferences (Sevastopol, 11–15 September, 2017). – 2017. – Vol. 129. – P. 03022.

13. Skatkov, A. V. Adaptive vulnerability detection model for unmanned vehicles drugs based on artificial immune systems / A.V. Skatkov, A.A. Bryukhovetskiy, D.V. Moiseev // IOP Conference Series: Materials Science and Engineering (Krasnoyarsk, 18–21 November, 2019). – Krasnoyarsk : Institute of Physics and IOP Publishing Limited, 2020. – P. 12028.

14. Moiseev, D. V. Intelligent decision - making support on the level of encryption of information transmitted in the UMV information exchange channels / D.V. Moiseev, A.A. Bryukhovetskiy, A.V. Skatkov // IOP Conference Series: Materials Science and Engineering (Krasnoyarsk, 18–21 November 2019). – Krasnoyarsk : Institute of Physics and IOP Publishing Limited, 2020. – P. 12086.

15. Agiwal, M. Next Generation 5G Wireless Networks: A Comprehensive Survey / M. Agiwal, A. Roy, N. Saxena //

IEEE Communications Surveys Tutorials. – 2016. – Vol. 18, No. 3. – P. 1617–1655.

16. Адаптивный метод обнаружения уязвимостей интерфейсов беспилотных транспортных средств в инфраструктуре умного города / А.В. Скатков, А.А. Брюховецкий, Д.В. Моисеев, В.И. Шевченко // Инфокоммуникационные технологии. – 2020. – Т. 18, № 1. – С. 45–50.

17. Мера Кульбака в задачах динамической кластеризации наблюдений состояния окружающей среды / А.В. Скатков, А.А. Брюховецкий, Д.В. Моисеев, Ю.Е. Шишкин // Системы контроля окружающей среды. – 2019. – № 3 (37). – С. 35–38.