УДК 004.056:061.68

Ю.А. Брюхомицкий

МОНИТОРИНГ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ МЕТОДАМИ ИСКУССТВЕННЫХ ИММУННЫХ СИСТЕМ*

Рассматривается задача мониторинга информационных процессов в компьютерных системах с целью их классификации на легитимные и нелегитимные процессы с применением аппарата искусственных иммунных систем. Поставленная задача решается на основе используемого в искусственных иммунных системах алгоритма отрицательного отбора. Отмечается, что важной особенностью такого решения является его высокая вычислительная трудоемкость, которая обусловлена экспоненциальным ростом числа детекторов, необходимых для реализации алгоритма отрицательного отбора, в зависимости от размерности задачи. Делается вывод о необходимости разработки более эффективных модификаций алгоритма отрицательного отбора.

Мониторинг информационных процессов; распознавание, классификация; искусственные иммунные системы; алгоритм отрицательного отбора; вычислительная трудоемкость.

Y.A. Bryukhomitsky

MONITORING INFORMATION PROCESSES METHODS OF ARTIFICIAL IMMUNE SYSTEM

The problem of monitoring information processes in computer systems for the purpose of classification for legitimate and illegitimate use of the machine with artificial immune systems. The problem is solved on the basis used in artificial immune systems, negative selection algorithm. It is noted that an important feature of this solution is its high computational complexity, which is caused by the exponential growth in the number of detectors required for the negative selection algorithm, depending on the dimension of the problem. It is concluded that a more effective modification of negative selection algorithm.

Monitoring of information processes; recognition; classification; artificial immune system; negative selection algorithm; computational complexity.

В информационных технологиях все большее внимание специалистов привлекает новое направление искусственного интеллекта – искусственные иммунные системы (Artificial Immune Systems), – которое основывается на использовании фундаментальных знаний в области иммунологии для решения прикладных задач [1].

В сфере компьютерной безопасности искусственные иммунные системы (ИИС) могут применяться для решения задач [2]:

- выявления неавторизованного использования информационных ресурсов;
- выявления вторжений (атак) на информационные системы;
- выявления аномалий в информационных процессах;
- поддержания целостности данных;
- подавления процессов распространения вредоносных программ;
- управления инцидентами информационной безопасности и др.

Значительная часть из перечисленных задач сводится, по существу, к проблеме нахождения отличий «своего» от потенциально опасного «чужого». В технической постановке это широко распространенные задачи распознавания и классификации образов.

* Работа выполнена при поддержке гранта РФФИ 12-07-00081-а.

При решении задач распознавания и классификации традиционными методами и средствами образы обычно описываются и выступают как целостные информационные комплексы, представленные в многомерном пространстве обучающих данных. Распознавание осуществляется централизованно, на системном уровне с применением различных методов сопоставления неизвестных образцов с эталонными образцами в пространстве обучающих данных. Для этого используются, в частности, геометрические методы определения меры близости (Хэмминга, Евклида, Махаланобиса и др.), параметрические методы, статистические методы, аппарат искусственных нейронных сетей и др. Точность решения задачи распознавания этими методами принципиально ограничена, если имеет место высокая вариативность образов, не позволяющий выполнить их точное описание. Принятие решения об отнесении неизвестного образца к одному или другому классу осуществляется лишь по окончанию всего цикла сопоставления образцов, что во многих случаях может оказаться уже запоздалой реакцией.

Решение задач распознавания и классификации с использованием подхода ИИС существенно отличается от традиционных подходов. Для этого используется другое представление и описание образов, другие методы сопоставления образцов, другие методы обработки данных и принятия решения. Как следствие, существенно другими становятся и свойства систем распознавания на основе ИИС, которые могут быть полезны и продуктивно использованы в сфере информационной безопасности.

Иммунная система живого организма осуществляет регулирование его взаимоотношений с внешней средой в сфере микробиологической безопасности. Она организует многоуровневую защиту организма от чужеродных клеток – антигенов. Основное ее свойство заключается в способности к выявлению антигенов и организации с помощью специальных клеток организма − иммуноцитов иммунного ответа, сводящегося к разрушению или нейтрализации антигенов. Ключевым механизмом появления такой способности у иммуноцитов является отрицательный отбор − сложный физико-химический процесс распознавания антигенов. Суть его в том, что иммуноциты, которые вступают в реакцию с собственными белками, уничтожаются, а остальные становятся чувствительными к антигенам. Циркулируя затем по всему организму, они выполняют функцию защиты от чужеродных клеток. При обнаружении «чужих» включаются механизмы нейтрализации и разрушения антигенов [3]. Причем принятие такого решения опосредовано коллективными действиями клеток иммунной системы без прямого вмешательства верхних отделов нервной системы организма.

С позиции информатики иммунная система интересна тем, что способна эффективно обрабатывать значительные объемы данных, используя для этого сложные высоко параллельные распределенные вычисления. При этом поведение иммунной системы в целом определяется большой совокупностью локальных взаимодействий. Попытки использовать эти принципы для решения разнообразных задач в области информационных технологий, в т.ч. информационной безопасности и привели к появлению ИИС. В отличие от традиционных информационных систем ИИС выполняют полностью децентрализованную обработку, в том числе и при решении задач распознавания.

Наиболее распространенной иммунологической моделью ИИС, применяемой в сфере компьютерной безопасности является алгоритм отрицательного отбора (АОО) [4, 5], который в самом общем виде формулируется следующим образом:

- определяется понятие «свой», как нормальная динамика поведения системы, которая описывается множеством строк символов фиксированной длины;

- создается набор детекторов «произвольных чужих», каждый из которых не должен совпадать с любой строкой нормальной совокупности строк символов «своего». При этом используется правило частичного совпадения, согласно которому две строки совпадают тогда и только тогда, когда они идентичны в определенном числе смежных позиций;
- производится непрерывное сопоставление новых поступлений строк в систему с детекторами. В случае совпадении строки с одним из детекторов она классифицируется как представитель «чужого».

Поставим задачу организации мониторинга информационных процессов в компьютерной системе с целью обнаружения присутствия нелегитимных процессов («чужих»), представляющих потенциальную угрозу нарушения информационной безопасности. Суть такого мониторинга сводится к решению задачи классификации протекающих информационных процессов на два класса: «свои» и «чужие». Поставленную задачу будем решать с использованием основных принципов и механизмов ИИС.

Пусть в компьютерной системе в нормальном состоянии может протекать $k = 1, 2, \ldots, M$ легитимных («своих») информационных процессов $P^k(t)$. В процессе функционирования компьютерной системы возможно появление нелегитимных информационных процессов («чужих») – $P^{\text{ч}}(t)$, представляющих потенциальную угрозу нарушения информационной безопасности. Задача мониторинга состоит в том, чтобы своевременно обнаружить появление среди протекающих процессов $P(t)$ нелегитимных процессов $P^{\text{ч}}(t)$.

Формализуем решение этой задачи при условии использования АОО в его классическом виде.

Первый пункт АОО сводится к специальному построчному представлению информационных процессов $P(t)$ и последующей регистрации легитимных процессов $P^k(t), k = \overline{1, M}$ путем формировании для каждого из них соответствующего шаблона.

Представим информационные процессы $P(t)$ конечными последовательностями событий: $P(t_i) = p_1, p_2, \ldots, p_i, \ldots, p_N, i = \overline{1, N}$. При этом $k = \overline{1, M}$ легитимным процессам будет соответствовать совокупность конечных последовательностей $P^k(t_i),\ i = \overline{1, N_k}$. Конкретный вид представления и кодирования отдельных событий $p_1, p_2, \ldots, p_i, \ldots, p_N$ процессов $P(t_i)$ определяется приложением. В большинстве приложений информационной безопасности события $p_1, p_2, \ldots, p_i, \ldots, p_N$ процесса $P(t_i)$ могут быть представлены символами $a_1, a_2, \ldots, a_i, \ldots, a_N$ некоторого алфавита $\boldsymbol{A}$, кодирующими эти события в числовой форме. Количество символов d алфавита $\boldsymbol{A}$, очевидно, будет соответствовать диапазону изменения чисел в каждой позиции последовательностей $a_1, a_2, \ldots, a_i, \ldots, a_N$, а, следовательно, – перечню всех возможных событий процессов $P(t_i)$.

Для определенности положим, что числовые значения $a_1, a_2, \ldots, a_i, \ldots, a_N$, кодирующие события процессов $P(t_i)$, представлены действительными числами, нормированными к фиксированному диапазону $d = (\min a_i, \max a_i)$, определяемому приложением. Для реализации в АОО операции сопоставления символов $a_1, a_2, \ldots, a_N$ по принципу частичного соответствия диапазон d удобно представлять m-разрядным двоичным кодом. При этом разрядность m задает точность двоичного представления исходного действительного числа. Очевидно, m-разрядным двоичным кодом можно закодировать 2^m чисел от 0 до $2^m–1$. При этом весь диапазон $d = (\min a_i, \max a_i)$ будет содержать $2^m–2$ интервалов. Соответственно размер интервала равен $\delta = (\min a_i, \max a_i) / (2^m–2)$. В таком случае величина a_i, изменяющаяся в диапазоне $\min a_i \le a_i \le \max a_i$, где $\max a_i = \min a_i + (2^m–2)\cdot d$, может быть отнесена к одному из интервалов $\delta_j, j = 1, 2, \ldots, (2^m–2)$ всего диапазона d с абсолютной ошибкой δ и представлена двоичным кодом номера интервала δ_j.

В том случае, если значения a_i по каким-либо причинам выходят за пределы нормированного интервала d, то эти значения следует исключить из анализа. Например, если $a_i < \min a_i$, то двоично-кодированное значение a_i будет состоять из одних нулей, а если $a_i > \max a_i$, то двоично-кодированное значение a_i будет состоять из одних единиц. Обработка данных реализуется таким образом, что двоичные комбинации [00…0] и [11…1] из анализа исключаются.

Принцип кодирования событий информационных процессов $P(t_i),\ i = \overline{1, N_k}$ поясняет рис. 1.

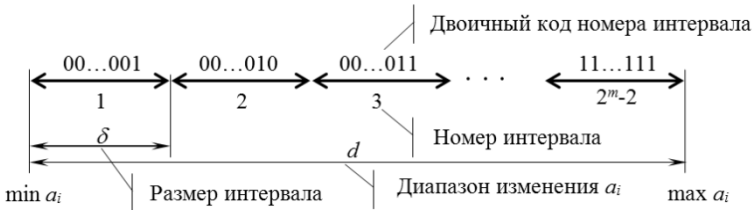

Рис. 1. Принцип кодирования событий информационных процессов

После описанного представления информационных процессов $P(t)$ в системе мониторинга возможно создание шаблонов легитимных информационных процессов $P^k(t_i)$, $k = \overline{1, M}$, $i = \overline{1, N_k}$, ориентированных на применение АОО.

Разобьем последовательности событий $p_1, p_2, \ldots, p_{N_k}$ каждого информационного процесса $P^k(t_i)$, представленные символами $a_1, a_2, \ldots, a_{N_k}$ алфавита $\boldsymbol{A}$, на множества строк равной длины по l событий в каждой строке. Для образования строк используем скользящее временное окно длиной l символов с шагом сдвига h символов. Каждое такое окно будет представлять порцию из l событий последовательности $p_1, p_2, \ldots, p_{N_k}$. В конечном итоге каждый легитимный информационный процесс $P^k(t_i)$, $k = \overline{1, M}$, $i = \overline{1, N_k}$ будет представлен набором из n строк по l событий в каждой строке. Каждый k-набор задает ориентированный на алгоритм отрицательного отбора шаблон легитимного процесса $P^k(t_i)$.

Вид шаблона одного легитимного информационного процесса при $l = 5$ и $h = 2$ показан на рис. 2.

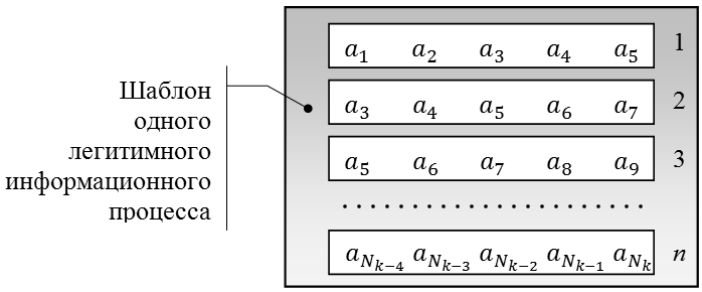

Рис. 2. Вид шаблона одного легитимного информационного процесса при l = 5 и h = 2

По описанному принципу формируются шаблоны для всей совокупности легитимных информационных процессов $P^k(t_i)$, $k = \overline{1, M}$.

Второй пункт АОО – это создание набора детекторов для обнаружения «чужих» информационных процессов $P^{\text{ч}}(t)$. В терминах систем распознавания образов его можно назвать этапом обучения системы мониторинга. Кандидаты в детекторы генерируются в виде строк длиной l символов. Числовые значения

$a_1, a_2, \dots, a_N$, кодирующие события $p_1, p_2, \dots, p_N$ информационных процессов $P^{\text{ч}}(t)$, генерируется случайно с равномерным законом распределения в заданном диапазоне *d*. Каждый образованный кандидат в детекторы поочередно сопоставляется со строками всех ранее сформированных $k = \overline{1, M}$ шаблонов легитимных информационных процессов $P^k(t_i)$ по принципу частичного совпадения. Детектор «чужого» не должен совпадать ни с одной строкой всех $k = \overline{1, M}$ шаблонов. В соответствии с принципом частичного совпадения две строки совпадают тогда и только тогда, когда они идентичны в *r* смежных позициях, где *r* – целочисленный параметр, выбираемый в зависимости от приложения. При установлении факта частичного совпадения соответствующий кандидат в детекторы уничтожается. Схема формирования набора детекторов «чужих» показана на рис. 3.

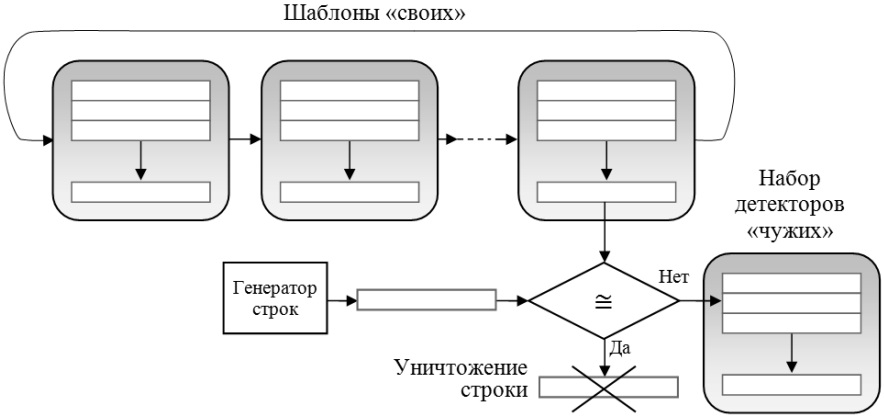

Рис. 3. Схема формирования набора детекторов

Параметр *r* имитирует свойство аффинности иммунной системы, т.е. – прочности связи между чужеродным агентом (антигеном) и антителом, вырабатываемым иммунной системой организма. В набор включаются только те детекторы, аффинность которых по сравнению со строками эталонов $k = \overline{1, M}$ меньше *r*. Процесс создания детекторов продолжается до тех пор, пока не будет сгенерировано их необходимое число. На этом процесс обучения системы заканчивается.

В рабочем режиме (режиме мониторинга) система функционирует в реальном масштабе времени и реализует третий пункт АОО. Все порожденные в компьютерной системе информационные процессы $P(t)$ сначала приводятся к виду, аналогичному представлению шаблонов легитимных информационных процессов $P^k(t_i)$, $k = \overline{1, M}$, а затем контролируются на предмет аномалий путем непрерывного сопоставления входящих в них строк с детекторами. Активация детектора свидетельствует о появлении аномальной строки, т.е. такого сочетания событий, которое отсутствовало в шаблонах легитимных информационных процессов $P^k(t)$, $k = \overline{1, M}$. В конечном итоге, это повышает вероятность появления в компьютерной системе «чужого» информационного процесса $P^{\text{ч}}(t)$.

Статистическую вероятность присутствия в компьютерной системе «чужого» информационного процесса $P^{\text{ч}}(t)$ можно отразить частотой срабатывания детекторов

$$p[P^{\text{ч}}(t)] \cong f = \frac{n^+}{n},$$

где $p[P^{\text{ч}}(t)]$ – статистическая вероятность появления «чужого» информационного процесса $P^{\text{ч}}(t)$; n^+– число положительных исходов сравнений строк; n – общее число проведенных сравнений строк.

Принятие решения о присутствии в компьютерной системе «чужого» информационного процесса $P^{\text{ч}}(t)$ в простейшем случае может быть принято по факту превышения частоты *f* некоторого порогового значения $f_{\text{п}}$:

$$P(t) \equiv \begin{cases} P^{\text{с}}(t), \text{если } f \le f_{\text{п}}; \\ P^{\text{ч}}(t), \text{если } f > f_{\text{п}}. \end{cases}$$

Причем, в соответствии с процедурой обучения, «чужим» будет признан любой процесс $P(t)$, отличающийся от всех процессов $P^k(t)$, $k = \overline{1,M}$.

Важным параметром, влияющим на качество и быстродействие системы мониторинга, является число детекторов N_D, необходимых и достаточных для своевременного обнаружения «нарушителя». В свою очередь, для получения детекторов в количестве N_D необходимо сгенерировать N_0 строк – кандидатов в детекторы.

Одна из возможных схем вероятностного расчета N_0 была представлена в работе [6] и используется здесь в качестве основы для интерпретации поставленной задачи.

Вероятность того, что случайная строка не совпадет с одним из шаблонов легитимных информационных процессов $P^k(t)$, $k = \overline{1,M}$, очевидно, можно определить как

$$p_M = (1 - p_s)^{M \cdot N_k}, \quad (1)$$

где p_s – вероятность совпадения двух случайно сгенерированных строк по правилу частичного соответствия.

Тогда необходимое число детекторов N_D определится как

$$N_D = N_0 \cdot p_M. \quad (2)$$

Вероятность того, что N_D детекторов не смогут обнаружить «чужой» информационный процесс соответствует ошибке второго рода, которую по аналогии с (1) можно определить как

$$p_2 = (1 - p_s)^{N_D}. \quad (3)$$

Из (3) следует, что

$$N_D = \log_{(1-p_s)} p_2 = \frac{\ln p_2}{\ln(1-p_s)} \cong -\frac{\ln p_2}{p_s}. \quad (4)$$

Соответственно

$$N_0 \cong \frac{N_D}{p_M} = -\frac{\ln p_2}{p_s \cdot p_M} = \frac{\ln p_2}{p_s(1-p_s)^{M \cdot N_k}}. \quad (5)$$

Для практического использования формулы (5) необходимо знать вероятность совпадения двух случайно сгенерированных строк p_s, которую для заданных параметров d, r, h можно приближенно рассчитать по формуле

$$p_s \cong k \cdot d^{-r}, \quad (6)$$

где

$$k = \left[\frac{h(d-1)}{d} + 1\right]. \quad (7)$$

Таким образом, число детекторов N_D, необходимое для обнаружения «чужого» с вероятностью p_2, потребует генерации N_0 строк – кандидатов в детекторы, которое можно определить по формулам.

Анализ формул (5)–(7) позволяет выявить характер зависимостей $N_D = f(p_2)$, $N_D = f(h)$, $N_D = f(d)$, $N_D = f(r)$.

Зависимость $N_D = f(p_2)$ при заданной постоянной величине p_s сводится к логарифмической зависимости $f(p_2) = \ln p_2$. При изменении вероятности p_2, как ошибки второго рода, в диапазоне ($1{,}0 \cdot 10^{-1}$ – $1{,}0 \cdot 10^{-5}$) изменяет N_D лишь в 5 раз. То есть вероятность p_2 в иммунологической схеме распознавания очень мало влияет на оценки N_D и N_0.

Зависимость $N_D = f(h)$ при прочих равных условиях сводится к изменению размера множителя k (в квадратных скобках) в выражении (6). Можно предположить, что для реальных задач в области компьютерной безопасности количество символов *d*

алфавита **A**, соответствующее перечню всех возможных событий процессов $P^k(t_i)$, ограничено диапазоном значений 10–1000, а для большинства реальных практических приложений лежит в диапазоне 20–100. Размер шага h сдвига символов в большинстве случаев лежит в диапазоне (1–3). Учитывая, что $d \gg h$, множитель $k \cong h + 1$. Из этого следует, что k, а, следовательно, и p_d линейно зависят от h.

Зависимости $N_D = f(d)$ и $N_D = f(r)$ являются наиболее чувствительными, так как параметры d и r связаны показательной функцией $p_s \cong k \cdot d^{-r}$, входящей в выражения (5) и (6) для определения N_D и N_0 соответственно. Поэтому число детекторов N_D и число строк, необходимых для их формирования N_0 определяются преимущественно параметрами d и r.

Для определения характера зависимости $N_D = f(d,r)$ представим ее в виде зависимости $N_D = f(p_s)$. Из выражений (4), (6) следует

$$N_D \cong -\frac{\ln p_2}{k \cdot d^{-r}} = -\frac{1}{k} \cdot \ln\, p_2 \cdot d^r. \quad (8)$$

Показательную функцию d^r, как известно, можно представить в виде экспоненты, в итоге получим:

$$N_D \cong= -\frac{1}{k} \cdot \ln\, p_2 \cdot e^{-r \cdot \ln d}. \quad (9)$$

То есть число детекторов N_R растет в экспоненциальной зависимости от параметров d и r шаблона «своего».

Зависимость $N_D = f(d,r)$ для значений d = 20, 50, 100 и r = 2, 3, 4 в виде графика показана на рис. 4.

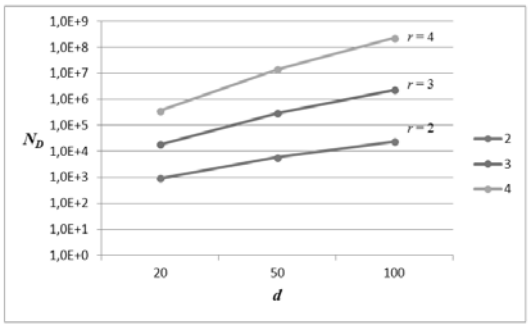

Рис. 4. Графики зависимостей $N_D = f(d,r)$

Расчет вероятности p_M как функции от полученных выше значений вероятностей p_s при заданном произведении $M{\cdot}N_k$ = 20000 позволяет в конечном итоге получить зависимости $N_D = f(p_s)$ и $N_0 = f(p_s)$, приведенные в виде графиков на рис. 5.

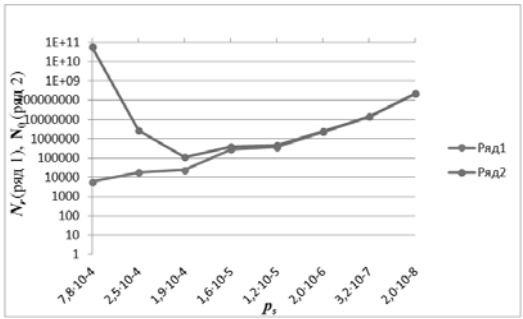

Рис. 5. Графики зависимостей $N_D = f(p_s)$, $N_0 = f(p_s)$

Анализ проведенных расчетов позволяет сделать следующие выводы.

1. Важнейшими характеристиками, определяющими качество мониторинга информационных процессов методами ИИС, являются число детекторов N_D для обнаружения «чужих» и число строк N_0, необходимое для их формирования.

2. Характеристики N_D и N_0, в свою очередь, определяются параметрами p_2, h, d, r, выбираемыми на стадии проектирования системы мониторинга в зависимости от решаемой задачи.

3. Функции $N_D = f(p_2)$, $N_D = f(h)$, $N_D = f(d)$, $N_D = f(r)$ имеют принципиально разный характер зависимостей от параметров p_2, h, d, r:

- функция $N_D = f(p_2)$ имеет логарифмическую зависимость от p_2;
- функция $N_D = f(h)$ имеет линейную зависимость от h;
- функция $N_D = f(d)$ имеет степенную зависимость от d;
- функция $N_D = f(r)$ имеет показательную зависимость от r.

Разный характер зависимостей $N_D = f(p_2)$, $N_D = f(h)$, $N_D = f(d)$, $N_D = f(r)$ определяют и разную (возрастающую) степень влияния параметров p_2, h, d, r на характеристики N_D и N_0.

4. Функция $N_0 = f(p_s)$ имеет экстремальную точку $N_0 = \min f(p_s)$, в которой число генерируемых строк N_0, необходимое для формирования N_D детекторов при определенном сочетании параметров p_2, d, r, h оказывается минимальным.

5. В большинстве практических приложений сочетание задаваемых параметров p_2, d, r, h приводит к экспоненциальному росту N_D и N_0.

Рассмотренный принцип реализации мониторинга информационных процессов в компьютерных системах методами искусственных иммунных систем с применение алгоритма отрицательного отбора показывает высокую вычислительную трудоемкость такой схемы. Сложность эта обусловлена, прежде всего, экспоненциальным ростом необходимых для реализации АОО числа детекторов в зависимости от размерности задачи. Поэтому дальнейшие исследования в этой прикладной области будут направлены на модификацию АОО в направлении снижения его вычислительной трудоемкости.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Искусственные иммунные системы и их применение / Под ред. Д. Дасгупты: Пер. с англ. / Под ред. А.А. Романюхи. – М.: Физматлит, 2006. – 344 с.
2. *Брюхомицкий Ю.А.* Использование принципов построения и функционирования иммунных систем в компьютерной безопасности / Материалы XII Международной научно-практической конференции «Информационная безопасность». Ч. I. – Таганрог: Изд-во ТТИ ЮФУ, 2012. – С. 3-10.
3. *Kuby J. Immunology. W.H.* Freeman and Co., 2nd edition, 1994.
4. *Forrest S., Perelson A.S., Allen L., Cherukuri R.* Self-nonself discrimination in a computer // In: Proc. of Ieee symposium on research in security, Oakland, CA, 16-18 May 1994. – P. 202-212.
5. *Dasgupta D., Forrest S.* Tool breakage detection in milling operations using a negative-selection algorithm // Technical report CS95-5, Department of computer science, University of New Mexico, 1995.
6. *Васильев В.И.* Интеллектуальные системы защиты информации: Учеб. пособие. – М.: Машиностроение, 2010. – 163 с.

Статью рекомендовал к опубликованию к.т.н. М.Ю. Руденко.

Брюхомицкий Юрий Анатольевич – Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Южный федеральный университет»; e-mail: bya@tsure.ru; 347928, г. Таганрог, ул. Чехова, 2; тел.: 88634371905; кафедра безопасности информационных технологий; доцент.

Bryukhomitsky Yuri Anatol'evich – Federal State-Owned Autonomy Educational Establishment of Higher Vocational Education "Southern Federal University"; e-mail: bya@tsure.ru; 2, Chekhova street, Taganrog, 347928, Russia; phone: +78634371905; the department of security in data processing technologies; associate professor.

УДК 004.056.5 004.89

В.С. Аткина

МОНИТОРИНГ СОСТОЯНИЙ КАТАСТРОФОУСТОЙЧИВОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ С ПОМОЩЬЮ ГИБРИДНОЙ ИММУННОЙ СЕТИ

Цель исследования: разработка методики классификации состояний катастрофоустойчивой системы с использованием гибридной иммунной сети. В рамках данного исследования решены следующие задачи: обоснована значимость обеспечения катастрофоустойчивости информационной системы в процессе управления информационной безопасностью организации в целом; предложен подход к процессу проведения мониторинга и контроля за показателями катастрофоустойчивости системы. Разработана и формально описана гибридная иммунная сеть, с применением алгоритмов клонального и «положительного» отбора и областью покрытия, образованной двумя типами детекторов. Сделан вывод о возможности применения разработанного подхода в процессе анализа катастрофоустойчивости информационных систем.

Катастрофоустойчивость; информационные системы; искусственная иммунная сеть; клональный отбор; «положительный» отбор; мониторинг; информационная безопасность.

V.S. Atkina

MONITORING THE STATES OF INFORMATION SYSTEM DISASTER RECOVERY WITH A HYBRID IMMUNE NETWORK

The purpose of the study is development of technique classification states of disaster recovery systems using a hybrid immune network. This study addressed the following objectives: to substantiate the importance of ensuring disaster recovery information system in the management of information security in general, the approach to the process of monitoring and performance monitoring disaster recovery system. The hybrid immune network is developed and formally described, using algorithms clonal and "positive" selection and coverage area formed by the two types of detectors. The conclusion about possibility of using the developed approach in the analysis of information systems disaster recovery.

Disaster recovery; information system; artificial immune network; positive selection algorithm; clonal algorithm; monitoring; information security.

На сегодняшний день все более необходимым и актуальным для успешного функционирования любой организации вне зависимости от принадлежности ее к государственному или частному сектору экономики является обеспечение непрерывности выполнения ее бизнес-процессов и защита информации от уничтожения, что достигается с помощью информационных систем (ИС) с высокими показателями доступности и катастрофоустойчивости. При этом важным этапов в процессе управления информационной безопасностью организации в целом будет являться деятельность, направленная на проведение периодического и своевременного контроля над текущим состоянием катастрофоустойчивости ИС и выработки по его результатам своевременных катастрофоустойчивых решений, позволяющих скорректировать текущие показатели катастрофоустойчивости.