9. *Домарев В.В.* Безопасность информационных технологий. Методология создания систем защиты. – 2-е изд. перераб. – Киев: ООО «ТИД «ДС», 2008. – 286 с.
10. *Жукова М.Н. Золотарев А.В.* Применение нечеткой логики при решении задачи комплексной оценки защищенности автоматизированных систем // В мире научных открытий: научное периодическое издание. – 2011. – Вып. 12. – С. 205-214.

Статью рекомендовал к опубликованию к.т.н., доцент П.М. Гофман.

Жукова Марина Николаевна – ФГБОУ ВПО «Сибирский государственный аэрокосмический университет им. академика М.Ф. Решетнева»; e-mail: mariem@inbox.ru; 660014, г. Красноярск, проспект им. газеты «Красноярский рабочий», 31; тел.: +79029101502; кафедра безопасность информационных технологий; к.т.н.; доцент.

Коромыслов Никита Андреевич – e-mail: koromyslov_nikit@list.ru; тел.: 83912621847; аспирант.

Zhukova Marina Nikolaevna – Siberian State Aerospace University; e-mail: mariem@inbox.ru; 31, prospekt imeni gazety «Krasnoyarskiy rabochiy», Krasnoyarsk, 660014, Russia; phone: +79029101502; the department of information technologies security; cand. of eng. sc.; associate professor.

Koromyslov Nikita Andreevich – e-mail: koromyslov_nikit@list.ru; phone: +73912621847; postgraduate student.

УДК 681.324

Ю.А. Брюхомицкий

МОДЕЛЬ АДАПТИВНОЙ САМООРГАНИЗУЮЩЕЙСЯ ИСКУССТВЕННОЙ ИММУННОЙ СИСТЕМЫ ДЛЯ РЕШЕНИЯ ЗАДАЧ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ*

Рассматриваются новые подходы и принципы построения искусственной иммунной системы (ИИС), отличающейся от известных тем, что в ней воспроизводятся способности к адаптации и самоорганизации, присущие иммунной системе живых организмов. Предлагаются новые подходы к моделированию свойства двойной пластичности, основанные на использовании различных механизмов формирования и регулирования численности детекторов. В процессе функционирования ИИС детекторы градуируются по эффективности обнаружении «чужих». Также вводится механизм регулирования баланса способностей ИИС к обнаружению ранее встретившихся и новых «чужих». В конечном итоге функционирование ИИС проявляет свойства параметрической и структурной пластичности. Параметрическая пластичность реализуется на стадии предварительного обучения и заключается в выборе исходных параметров представления и кодирования информационных процессов, реализации процедуры создания шаблонов и формирования первичного набора детекторов. Структурная пластичность реализуется на стадии рабочего функционирования в «духе коллективизма» путем выявления и замены слабейших элементов новыми, удаления бесполезных элементов, заполнения ниш, не занятых имеющимися элементами. В конечном итоге в отличие от известных ИИС проявляет присущий живой иммунной системе комбинированный характер функционирования: экзогенный в части защиты от внешних нарушителей и эндогенный в части обеспечения постоянства и целостности внутренней среды и поддержания механизмов внутренней коммуникации.

Искусственная иммунная система; адаптация; самоорганизация; обнаружение «чужих» информационных процессов; свойства параметрической и структурной пластичности.

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

Yu.A. Bryukhomitsky

ADAPTIVE SELF-ORGANIZING ARTIFICIAL IMMUNE SYSTEM MODEL FOR A COMPUTER SECURITY PARTICULAR PURPOSE

New approaches and principles of artificial immune system (AIS) building are considered, which differs from prior ones in that it reproduces the ability to adapt and self-organization that is appropriate to immune system of living organisms. There are new approaches to the property of double-plasticity modeling proposed, which based on the use of different mechanisms of detectors number formation and regulation. While the AIS operating, detectors are calibrated by the effectiveness of finding the "strangers". It also introduces a mechanism for regulating the balance of AIS capabilities to the discovery of new and previously encountered "strangers". At least, the AIS functioning get the properties of parametric and structural plasticity. The parametric plasticity is implemented on a pre-training stage and consists in selection of initial parameters for information processes representation and coding, realization of the templates creating procedure and creation of the primary set of detectors. The structural plasticity is implemented on the stage of active functioning in the "spirit of cooperation" by identifying and replacing the weakest elements by new ones, removing useless elements, filling the vacant niches, not occupied by the existing elements. Finally, in contrast to the well-known ones, AIS shows the complex functioning temper, inherent to living immune system: exogenous in protecting against external violators and endogenous in terms of ensuring of internal environment constancy and integrity and maintaining the mechanisms of internal communication.

Artificial immune system; adaptation; self-organization; detection of "strange" information processes; parametric and structural plasticity properties.

На технологии построения современных информационных систем сильное влияние оказали результаты биологических исследований живых организмов. В настоящее время это влияние представлено широким арсеналом методов и средств искусственного интеллекта, которые занимают все более прочные позиции в информатике, кибернетике, информационной безопасности. В первую очередь, это касается аппарата искусственных нейронных сетей, а также эволюционных и генетических алгоритмов, которые во многих случаях позволили кардинально изменить подходы к проектированию информационных систем. В конце прошлого века искусственный интеллект пополнился еще одной технологией, заимствованной из биологических исследований, – искусственными иммунными системами (ИИС) [1]. Однако, в отличие от искусственных нейронных сетей, эволюционных и генетических алгоритмов, ИИС пока не заняли прочного места в современных информационных технологиях. По мнению специалистов в этой области [1–3] это объясняется тем, что ИИС в своем нынешнем виде воспроизводят лишь самые общие принципы защиты организма от микробиологической опасности что, в конечном итоге, дает мало новых практических результатов при построении технических систем. Для получения более ощутимых результатов, возможно, следует рассматривать иммунную систему не только и не столько как систему защиты, а как самоотождествляющуюся систему, которая в условиях постоянного контакта с внешней средой подвергается постоянной внутренней реорганизации на структурном и параметрическом уровнях [2–7]. Параметрическая пластичность обеспечивается механизмом адаптации, позволяющего системе в ходе выполнения текущей задачи изменять параметры функционирования для повышения ее эффективности. Структурная пластичность дает системе новые возможности для адаптации. В системах взаимодействующих элементов она сводится к способности добавления новых и исключения уже имеющихся элементов. Эти два разных способа адаптации органично связаны и используются в одной системе. Иммунологи называют это свойство иммунной системы двойной пластичностью.

Важной особенностью иммунной системы, отличающей ее от технической системы, является различие причин проведения внутренних изменений. В технических системах изменения, как правило, носят экзогенный характер, являясь результатом взаимодействия с внешней средой. В иммунной системе изменения осуществляются на внутрисистемном уровне, и напрямую не зависит от внешних воздействий. Экзогенный характер иммунной системы проявляется лишь как системы защиты от внешних нарушителей. Именно эта сторона иммунной системы и воспроизводится, как правило, в ИИС, применяемой в сфере информационной безопасности. В то же время, взгляд на иммунную систему как на самоотождествляющуюся [3–7], функция которой состоит в поддержании некоторых механизмов внутренней коммуникации и обеспечении постоянства внутренней среды, свидетельствует об эндогенном характере ее функционирования.

Так, или иначе, желание получить от ИИС существенно более значительные результаты в инженерной практике и, в том числе, в сфере информационной безопасности, связано с комплексным подходом, включающим воспроизведение в ИИС как экзогенных, так и эндогенных принципов функционирования на основе моделирования свойств двойной пластичности. Первоначальные попытки моделирования этих свойств в ИИС, ориентированных на компьютерную безопасность, были уже предприняты в работах [8–10]. В настоящей работе рассматриваются новые подходы к моделированию свойства двойной пластичности в задачах, использующие различные методы формирования и регулирования численности детекторов.

Предлагается следующая обобщенная схема мониторинга информационных процессов в КС на основе адаптивной самоорганизующейся ИИС.

1. Фаза предварительного обучения ИИС.
   - 1.1. Специальное иммунологическое представление и кодирование информационных процессов.
   - 1.2. Создание шаблонов «своих».
   - 1.3. Создание набора первичных детекторов для обнаружения «чужих».
2. Рабочая фаза.
   - 2.1. Мониторинг информационных процессов.
   - 2.2. Организация подсчета числа случаев срабатывания каждого детектора (определение параметра статуса детекторов).
   - 2.3. Установление в общей численности детекторов границы «новизна / память», устанавливающей желаемый баланс способностей ИИС к обнаружению новых и сохранению памяти на уже встреченных «чужих».
   - 2.4. Работа механизма «новизна / память».
     - 2.4.1. До границы «новизна / память».
       - 2.4.1.1. Выбор и уничтожение ни разу не активировавшихся первичных детекторов.
       - 2.4.1.2. Генерация новых, вторичных детекторов, отличных от шаблонов «своих» и аффинных к детекторам с высоким статусом.
     - 2.4.2. После достижения границы «новизна / память».
       - 2.4.1.3. Выявление и уничтожение детекторов с самым низким ненулевым статусом.
       - 2.4.1.4. Генерация новых первичных детекторов, отличных от шаблонов «своих».

В обеих фазах функционирования общее число детекторов остается постоянным.

Детализируем представленную схему работы ИИС.

В компьютерной системе (КС) в разные моменты возможно присутствие двух видов информационных процессов: легитимных («своих») и нелегитимных («чужих»), представляющих потенциальную угрозу нарушения информационной безопасности. Число «своих» информационных процессов $P^k(t)$ определено и фиксировано: k = 1, 2, …, M. В ходе функционирования КС возможно появление «чужих» информационных процессов – $P^{ч}(t)$. Задача АСИИС состоит в своевременном обнаружении процессов $P^{ч}(t)$.

1. Фаза предварительного обучения ИИС

1.1. Специальное иммунологическое представление и кодирование информационных процессов. Все информационные процессы $P(t)$, протекающие в компьютерной системе, как «свои», так и «чужие» представляются конечными последовательностями событий: $P(t_i) = p_1, p_2, \dots, p_i, \dots, p_N, i = \overline{1, N}$. 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 $p_1, p_2, \dots, p_i, \dots, p_N$ процессов $P(t_i)$ определяется приложением. В большинстве приложений информационной безопасности события $p_1, p_2, \dots, p_i, \dots, p_N$ процесса $P(t_i)$ могут быть представлены символами $a_1, a_2, \dots, a_i, \dots, a_N$ некоторого алфавита $\boldsymbol{A}$, кодирующими эти события в числовой форме. Количество символов d алфавита $\boldsymbol{A}$ соответствует диапазону изменения чисел в каждой позиции последовательностей $a_1, a_2, \dots, a_i, \dots, a_N$, а, следовательно, – перечню всех возможных событий процессов $P(t_i)$.

Числовые значения $a_1, a_2, \dots, a_i, \dots, a_N$, кодирующие события процессов $P(t_i)$, в большинстве приложений компьютерной безопасности могут быть представлены действительными числами, нормированными к фиксированному диапазону d = (min a_i, max a_i), определяемому приложением.

Ключевой операцией в системе мониторинга информационных процессов является сопоставление символов процессов, представленных символами $a_1, a_2, \dots, a_N$ по принципу частичного совпадения. Для ее реализации диапазон d удобно представлять m-разрядным двоичным кодом, позволяющим 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 δ = (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)·d, может быть отнесена к одному из интервалов δ_j, j = 1, 2, …, (2^m–2) всего диапазона d с абсолютной ошибкой δ и представлена двоичным кодом номера интервала δ_j.

Более подробно принцип кодирования событий информационных процессов показан в работе [11].

1.2. Создание шаблона «своих». «Свои» информационные процессы $P^k(t_i)$, $k = \overline{1, M},\ i = \overline{1, N_k}$ регистрируются в системе путем формировании для каждого из них соответствующего шаблона. Для этого последовательности событий $p_1, p_2, \dots, p_{N_k}$ каждого информационного процесса $P^k(t_i)$, представленные символами $a_1, a_2, \dots, a_{N_k}$ алфавита $\boldsymbol{A}$, разбиваются на множества строк равной длины по l событий в каждой строке. Для образования строк используется скользящее временное окно длиной l символов с шагом сдвига h символов. Каждое такое окно будет представлять порцию из l событий последовательности $p_1, p_2, \dots, p_{N_k}$. 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 применение в ИИС шаблон легитимного процесса $P^k(t_i)$.

По описанному принципу формируются шаблоны $T^c = T_1^c, T_2^c, \dots, T_M^c$ для всей совокупности легитимных информационных процессов $P^k(t_i)$, $k = \overline{1, M}$. При этом каждый шаблон $T_k^c, k = \overline{1, M}$ состоит из N_k строк по l символов.

1.3. Создание первичного набора детекторов «чужих». Для обнаружения «чужих» информационных процессов $P^{\text{ч}}(t)$ вначале создается набор кандидатов в первичные детекторы $D_1^1, D_2^1, \dots, D_{N_0}^1$. Кандидаты в первичные 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 первичные детекторы $D_1^1, D_2^1, \dots, D_{N_0}^1$ поочередно сопоставляется со строками всех ранее сформированных шаблонов $T^c = T_1^c, T_2^c, \dots, T_M^c$ легитимных информационных процессов $P^k(t_i)$ по принципу частичного совпадения. Создаваемый первичный детектор не должен совпадать ни с одной строкой всех $k = \overline{1, M}$ имеющихся шаблонов «своих». В соответствии с принятым в иммунологическом алгоритме отрицательного отбора (АОО) 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.

Параметр r имитирует свойство аффинности иммунной системы – прочности связи между чужеродным агентом (антигеном) и антителом, вырабатываемым иммунной системой организма. В набор включаются только те первичные детекторы, аффинность которых по сравнению со строками эталонов $k = \overline{1, M}$ меньше r.

При установлении факта частичного совпадения соответствующий кандидат в первичные детекторы уничтожается. Оставшиеся после уничтожения строки образуют множество первичных детекторов $D^1 = D_1^1, D_2^1, \dots, D_N^1$, которые предназначены для распознавания «чужих». Процесс создания первичных детекторов продолжается до тех пор, пока не будет сформировано их необходимое число N. На этом процесс обучения системы заканчивается. Число первичных детекторов N является важным параметром, определяющим основные характеристики ИИС. Выбор этого параметра зависит от приложения и может быть реализован различными способами. Наиболее приемлемым представляется первоначальный ориентировочный расчет N для обеспечения желаемых характеристик приложения (точности и быстродействия), например, по схеме, приведенной в работах [11, 12], с последующим его уточнением N в процессе пробной эксплуатации ИИС.

2. Рабочая фаза ИИС

2.1. Распознавание «чужих». Все порожденные в КС информационные процессы $P(t_i)$, $i = \overline{1, N}$, представленные в соответствии с п. 1.1 алгоритма, контролируются на предмет аномалий путем 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 $P^k(t)$, $k = \overline{1, M}$. Степень отклонения аномальной строки от шаблона «своего» определяется параметром аффинности r. Появление аномальной строки создает прецедент, свидетельствующий о возможной угрозе нарушения информационной безопасности.

Принятие решения о наличии или отсутствии в КС нелегитимных информационных процессов $P^{\text{ч}}(t)$ может быть реализовано по-разному в зависимости от характера приложения и принятой в КС политики безопасности. Представляется возможным использование двух типов правил принятия решения «жесткого» или «мягкого»:

- *«жесткое»* решающее правило: ответ «это – чужой» формируется сразу же после срабатывания любого детектора, что соответствует обнаружению в неизвестном информационном процессе $P^x(t)$ строки, отсутствующей в шаблоне легитимных информационных процессов;
- *«мягкое»* решающее правило: ответ «это – чужой» формируется при превышении частоты срабатывания детекторов некоторого порогового значения, что соответствует превышению в неизвестном информационном процессе $P^x(t)$ допустимой частоты появления строк, отсутствующих в шаблоне легитимных информационных процесса.

Правила принятия решения фактически задают допустимое количество совпадений строк неизвестного процесса с детекторами. Превышение этого количества классифицирует неизвестный процесс $P^x(t_i)$ как «чужой». Математическая формулировка этих правил приведена в работе [9].

2.2. Определение статуса детекторов. В течение рабочей фазы функционирования АСИИС каждый из первичных детекторов множества $D^1 = D_1^1, D_2^1, \dots, D_N^1$ за период *T* своего функционирования с момента начала рабочей фазы t_0 и до текущего момента t_i будет в разной степени участвовать в принятии решения «свой – чужой». Одни детекторы срабатывали чаще, другие срабатывали реже, третьи не срабатывали вообще. При каждом срабатывании того или иного детектора система принимала определенное решение: «свой» или «чужой».

Положим, что по окончании этапа 1.3 всем созданным первичным детекторам D^1 в качестве начального присвоен нулевой статус $S_{D_j^1} = 0,\ j = 1, 2, \dots, N$.

Будем полагать, что в распоряжении ИИС имеется система аудита, фиксирующая события безопасности, путем анализа которых апостериори можно установить достоверность принятых ИИС решений «свой – чужой». Используя эту информацию, можно создать механизм управления статусом каждого детектора, функционирующий следующим образом.

При использовании в системе «жесткого» решения. Если по очередному прецеденту ИИС приняла решение «это чужой», и это решение по данным аудита было правильным, то соответствующий сработавший первичный детектор D_j^1 повышает свой статус на единицу: $S_{D_j^1} = S_{D_j^1} + 1$. Если по очередному прецеденту АСИИС приняла решение «это свой», и это решение по данным аудита было правильным, то соответствующий сработавший первичный детектор D_j^1, «ответственный» за это решение понижает свой статус на единицу: $S_{D_j^1} = S_{D_j^1} - 1$.

При использовании в системе «мягкого» решения. Изменение статуса производится по тому же принципу, но не одного первичного детектора D_j^1, а группе $D_1^1, D_2^1, \dots, D_L^1$, состоящей из L первичных детекторов, по результатам срабатывания которых было принято соответствующее решение: $S_{D_k^1} = S_{D_k^1} \pm 1,\ k = 1, 2, \dots, L$.

Результатом работы такого механизма будет динамический процесс, протекающий за период *T* рабочей фазы ИИС, в котором определяются текущие значения статуса первичных детекторов в виде целых чисел со знаком, включая 0.

Теперь производится операция сортировки всех значений статуса $S_{D_j^1},\ j = 1, 2, \dots, N$ первичных детекторов от минимального до максимального. В случае возможных совпадений статуса нескольких первичных детекторов, они располагаются группой в порядке возрастания номера детектора $j = 1, 2, \dots, N$. В результате получим отсортированный по возрастанию статуса $S_{D_\propto^1}$ список первичных детекторов $D_\propto^1 = D_1^1, D_2^1, \dots, D_N^1,\ \propto = 1, 2, \dots, N$. Пример списка отсортированных по статусу 100 первичных детекторов приведен на рис. 1, а гистограмма их распределения по статусу приведена на рис. 2.

Статус первичных детекторов	-5	-4	-3	-2	-1	0	1	2	3	4	5
Число первичных детекторов	0	1	3	4	6	50	10	9	7	5	5

Рис. 1. Пример списка отсортированных по статусу 100 первичных детекторов

Рис. 2. Гистограмма распределения 100 первичных детекторов по статусу

2.3. Установление границы «новизна / память». Смысл функционирования самоорганизующейся ИИС состоит в установлении и поддержании разумного баланса способностей:

- к обнаружению новых, ранее не встречавшихся «чужих»;
- к сохранению в памяти условий обнаружения уже встретившихся «чужих».

Обеспечение указанного баланса в ИИС реализуется путем регулирования численности двух видов детекторов: тех, которые в процессе функционирования системы уже активировались и тех, которые еще не активировались. Первые реализуют иммунологическую память на ранее встретившихся «чужих», вторые создают потенциальную способность к обнаружению новых, ранее не встречавшихся «чужих».

При условии сохранения определенного уровня сложности и производительности системы, очевидно, что указанный баланс может обеспечиваться только на основе ограничения общей численности детекторов и поддержания ее на некотором постоянном уровне.

В таких условиях и ограничениях целесообразно для каждой конкретной реализации ИИС априори установить желаемый баланс указанных способностей в виде границы «новизна / память» между числом детекторов двух видов. Тогда включение механизма «новизна/память» разделит функционирование системы в рабочей фазе на два последовательных этапа: предшествующий достижению границы и последующий после достижения границы.

2.4. Работа механизма «новизна / память» начинается после появления в списке первого детектора, обнаружившего «чужого» и повысившего свой статус, и продолжается в течение всей фазы функционирования системы.

На первоначальном этапе, предшествующем достижению границы «новизна / память» работа механизма «новизна / память» сводится к двум подэтапам, выполняемым в любой последовательности:

- генерируется новый, вторичный детектор, отличный от шаблонов «своих», аффинный к детектору с самым высоким статусом;
- выбирается и уничтожается детектор с самым низким статусом.

Пусть при мониторинге очередное сравнение текущей строки $S_j = s_1, s_2, \dots, s_l$ событий $p_1, p_2, \dots, p_l$ информационного процесса $P(t_i)$ с первичным детектором D_k^1 создает прецедент, свидетельствующий о возможной угрозе нарушения информационной безопасности.

Согласно принятого в АОО принципу частичного совпадения две строки совпадают тогда и только тогда, когда они идентичны в r смежных позициях. Следовательно, в строке $S_j = s_1, s_2, \dots, s_l$ информационного процесса $P(t_i)$ всегда можно идентифицировать группу из r смежных символов ответственную за активацию первичного детектора D_k^1

$$G_j = s_{1+\Delta}, s_{2+\Delta}, \dots, s_{r+\Delta},$$

где $i = 1, 2, \dots, r$ – номер позиции символа в строке S_j; $(i + \Delta)$ – номер позиции символов в группе G_j; Δ – величина сдвига между начальным номером позиции символа в строке S_j и начальным номером позиции символа в группе G_j).

При условии, что проверка строк на частичное соответствие проводится только в соответствующих смежных позициях, вторичный детектор D_k^2 предлагается формировать по следующему алгоритму:

1°. В строке $S_j = s_1, s_2, \dots, s_l$ информационного процесса $P(t_i)$, вызвавшей активации первичного детектора D_k^1, идентифицируется соответствующая группа из r смежных символов $G_k = s_{1+\Delta}, s_{2+\Delta}, \dots, s_{r+\Delta}$.

2°. Генерируется кандидат во вторичные детекторы D_k^2 путем сдвига группы G_k вдоль строки S_j на некоторое число позиций с заполнением остальных позиций строки случайными значениями ξ_i в заданном диапазоне значений d.

3°. Как и при создании первичных детекторов, образованный кандидат во вторичные детекторы D_k^2 поочередно сопоставляется со строками всех ранее сформированных $k = \overline{1, M}$ шаблонов легитимных информационных процессов $P^k(t_i)$ по принципу частичного совпадения в r смежных позициях. При установлении факта такого совпадения соответствующий кандидат уничтожается и заменяется новым. Процедура продолжается до появления нового вторичного детектора D_k^2, не совпадающего с шаблонами «своих». Новому вторичному детектору D_k^2 присваивается нулевой статус, и он пополняет список первичных детекторов. Несмотря на то, что вторичный детектор имеет только нулевой статус, вероятность его активации на информационные процессы, близкие уже обнаруженному «чужому» при последующем функционировании системы будет повышена.

После удачного формирования вторичного детектора выбирается и уничтожается детектор с самым низким статусом.

Для рассмотренного примера уничтожается единственный детектор со статусом -4 (самый низкий статус) и появляется новый детектор с нулевым статусом, который пополняет соответствующую группу с 50 до 51. При этом число детекторов остается равным 100.

Со временем реализация первого этапа механизма «новизна / память» будет приводить к смещению рабочей точки в численности детекторов в направлении увеличения доли активированных детекторов, составляющих иммунологическую память на ранее обнаруженных «чужих», и уменьшения доли еще не активированных детекторов, составляющих, тем не менее, потенциальную возможность обнаружения новых «чужих».

Работа механизма «новизна / память» на последующем после достижения границы этапе также сводится к двум подэтапам, выполняемым в любой последовательности:

- генерируется новый первичный детектор, отличный от шаблонов «своих»;
- выявляется и уничтожается детектор с самым низким, не ненулевым статусом.

Процедура генерации нового первичного детектора ничем не отличается от изложенной выше в п. 3.1. Назначение этой процедуры – увеличение численности первичных детекторов, с целью обновления способности системы к обнаружению новых, ранее не встречавшихся «чужих». Для компенсации роста численности новых детекторов соответственно уничтожается ранее активировавший детектор с самым низким статусом. Логика выбора последнего обусловлена тем, что по должен быть уничтожен самый плохой детектор из числа уже участвовавших в обнаружении «чужих».

Для рассмотренного примера число детекторов с нулевым статусом становится равным 52, а число детекторов со статусом -3 уменьшается на единицу.

Непрерывное функционирование ИИС по описанной схеме со временем приведет к тому, что рабочая точка в соотношении численности детекторов достигнет заданной границы «новизна / память» и установится на ней окончательно.

Рис. 3 поясняет работу механизма «новизна / память» на последовательных стадиях структурной эволюции системы.

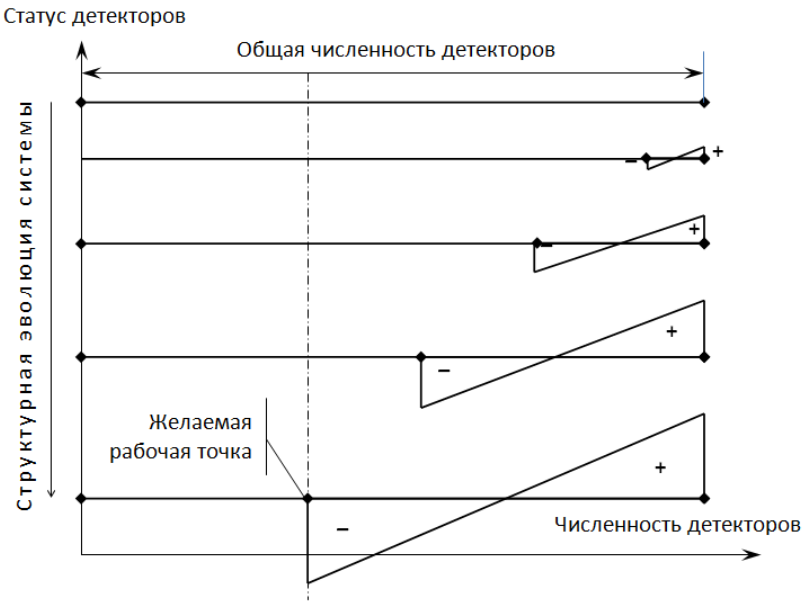

Рис. 3. Работа механизма «новизна/память» на последовательных стадиях эволюции системы

В конечном итоге функционирование такой ИИС будут содержать черты как параметрической, так и структурной пластичности.

Параметрическая пластичность ИИС реализуется на стадии предварительного обучения и заключается в выборе параметров:

- иммунологического представления и кодирования информационных процессов;

- реализации процедуры создания шаблонов;
- формирования и численности первичного набора детекторов «чужих».

Структурная пластичность ИИС реализуется на стадии рабочего функционирования в «духе коллективизма»:

- выявление и замена слабейших элементов новыми;
- удаление лишних, бесполезных элементов;
- заполнение ниш, не занятых имеющимися элементами.

Таким образом, описанная ИИС в отличие от известных проявляет искомый комбинированный характер функционирования: экзогенный в части защиты от внешних нарушителей и эндогенный в части обеспечения постоянства и целостности внутренней среды и поддержания механизмов внутренней коммуникации.

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. *Bersini H., Varela F.* Hints for adaptive problem solving gleaned from immune networks // Proc. 1st Conf. on Parallel Problem Solving from Nature (Eds. Ft.-P. Schwefel, R. Manner). Springer-Verlag, 1990. – P. 343-354.
3. *Bersini FI., Varela F.* The immune learning mechanisms: Recruitment reinforcement and their applications // Computing with biological metaphors (Ed. R. Patton). L.: Chapman and Hall, 1994.
4. *Detours V., Bersini H., Stewart J., Varela F.* Development of an idiotypic network in shape space // J. Theor. Biol. – 1994. – Vol. 170. – P. 401-414.
5. *Lundkvist I., Coutinho A., Varela F., Holmberg D.* Evidence for a functional idiotypic network among natural antibodies in normal mice // Proc. Natl. Acad. Sci. – 1989. – Vol. 86. – P. 5074-5078.
6. *Varela F., Coutinho A., Dupire B., Vaz N.* Cognitive networks: Immune, neural and otherwise. In: Theoretical Immunology, V. 2 (Ed. A. Perelson). SFI Series on the Science of Complexity. New Jersey: Addison Wesley, – 1988. – P. 359-375.
7. *Varela F.J., Coutinho A.* Second generation immune network // Immunol. Today. – 1991. – Vol. 12, № 5. – P. 159-166.
8. *Брюхомицкий Ю.А.* Предпосылки создания моделей компьютерной безопасности на принципах функционирования иммунных систем // Известия ЮФУ. Технические науки. – 2012. – № 1 (126). – С. 159-165.
9. *Брюхомицкий Ю.А.* Модель искусственной иммунной системы с двойной пластичностью // Материалы XIII Международной научно-практической конференции «Информационная безопасность». Ч. I. – Таганрог: Изд-во ЮФУ, 2013. – С. 147-155.
10. *Брюхомицкий Ю.А.* Регулирование распознающих свойств искусственных иммунных систем с двойной пластичностью // Материалы XIII Международной научно-практической конференции «Информационная безопасность». Ч. I. – Таганрог: Изд-во ЮФУ, 2013. – С. 155-161.
11. *Брюхомицкий Ю.А.* Мониторинг информационных процессов методами искусственных иммунных систем // Известия ЮФУ. Технические науки. – 2012. – № 12 (137). – С. 82-90.
12. *Васильев В.И.* Интеллектуальные системы защиты информации: учебное 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@tgn.sfedu.ru; 347928, г. Таганрог, ул. Чехова, 2; тел.: 88634371905; кафедра безопасности информационных технологий; доцент.

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