УДК 004.056.5, 004.89

СИСТЕМА АНАЛИЗА КАТАСТРОФОУСТОЙЧИВОСТИ

В.С. Аткина

Волгоградский государственный университет
E-mail: atkina.vladlena@yandex.ru

Описана проблема создания катастрофоустойчивых информационных систем и их значение при обеспечении информационной безопасности. Предположено, что при создании и сопровождении катастрофоустойчивых информационных систем необходимо проводить анализ текущих показателей катастрофоустойчивости системы и оценку эффективности катастрофоустойчивых решений. Предложена и формально описана система анализа катастрофоустойчивости, построенная на базе искусственной иммунной системы. На примере результатов проведенных экспериментальных исследований показана возможность применения предложенного решения в качестве инструментального средства поддержки принятия решений.

Ключевые слова:
Информационная система, катастрофоустойчивость, искусственные иммунные системы, катастрофоустойчивые решения, дестабилизирующие факторы, информационная безопасность.

Key words:
Information system, disaster recovery, artificial immune systems, disaster recovery solutions, destructive factors, information security.

На сегодняшний день деятельность любой организации (предприятия, учреждения) вне зависимости от принадлежности к государственной или коммерческой сфере тесно связана с использованием информации в различных ее видах, и, как правило, значительный процент информации представлен в электронном виде. Следовательно, процесс функционирования типовой организации состоит в постоянной обработке больших объемов информации, их анализе, принятии решений и управленческой деятельности. Для автоматизации данных процессов организацией используются информационные системы (ИС) различного типа. А это означает, что для успешного существования и развития организации необходимо обеспечивать безопасность ИС и циркулирующей в ней информации.

При этом одним из важнейших компонентов безопасности информации будет обеспечение доступности данных и надежности их обработки, что является особенно актуальным в настоящее время в связи с постоянным возникновением чрезвычайных ситуаций различного рода в самых различных областях человеческой деятельности. В соответствии с [1] к подобным чрезвычайным ситуациям можно отнести стихийные бедствия, имеющие самые различные последствия для всех сфер жизни общества (например, события в Японии 2011 г.), террористическую угрозу (особенно после известных событий 11 сентября 2001 г. в США), техногенные катастрофы. Анализ показывает, что все перечисленные угрозы, как правило, имеют комбинированный характер и приводят к возникновению и развитию зачастую неконтролируемого потока негативных последствий. В этих условиях обеспечение непрерывности бизнес-процессов, сохранности и доступности информации, а также повышение катастрофоустойчивости соответствующих производственных и ИС, входящих в состав современных организаций (в том числе и виртуальных), является одним из важнейших стратегических направлений развития экономики.

Создание катастрофоустойчивых информационных систем (КАИС) обеспечивается за счет внедрения специальных катастрофоустойчивых решений, представляющих собой комплекс организационно-технических мероприятий и планов поведения персонала в случае наступления катастрофы. Основной целью применения данных решений является обеспечение непрерывности функционирования ИС в условиях деструктивного воздействия, сокращение объемов потери данных и минимизация времени восстановления работоспособности ИС. При этом каждое из решений отличается своей стоимостью, временем внедрения и эффективностью. Поэтому для того чтобы определить, какое из решений или их сочетание будет наиболее выгодно организации-владельцу ИС по соотношению затрат на внедрение, стоимости информационных ресурсов и требований к уровню катастрофоустойчивости, необходимо провести анализ текущего состояния ИС; оценку катастрофоустойчивых решений и выбрать наиболее подходящие с учетом специфики каждой конкретной организации [2, 3].

Для решения поставленных задач автором предлагается система анализа катастрофоустойчивости, построенная на базе искусственной иммунной системы. Формально данную систему можно описать следующим кортежем:

$$M_{DRIS}=(\{M_{IS}\}, \{R_{DRIS}\}, \{DF\}, \{DRS\}, IMS),$$

где $\{M_{IS}\}$ – множество, описывающее КАИС, ее структуру, характеристики и показатели катастрофоустойчивости; $\{R_{DRIS}\}$ – множество требований организации-владельца к степени катастрофоустойчивости системы и потенциально возможным затратам; $\{DF\}$ – множество дестабилизирующих факторов существенной среды; $\{DRS\}$ – множество катастрофоустойчивых решений; IMS – функция управления процессом принятия решений, построенная на базе модели иммунной системы.

Множество, описывающее модель анализируемой КАИС в соответствии с [4], представляет собой

множество $\{M_{IS}\}=\{\{S\},\{C\},\{DRS\}\}$, где $\{S\}$ – множество состояний системы в различные периоды функционирования. Каждое состояние $S_i \in \{S\}$ описывается следующим кортежем $S_i=\{G_{is}, L, T_R, D_{class}, N_{Dlost}, Z\}$, где G_{is} – граф, описывающий физическую структуру КАИС; L – уровень катастрофоустойчивости, T_R – время восстановления функционирования; D_{class} – класс доступности (готовности); N_{Dlost} – объем потерянных данных; Z – живучесть; C – стоимость системы.

$\{DRS'\}$ – множество катастрофоустойчивых решений, уже внедренных (имеющихся) в КАИС на момент исследования, при этом следует учитывать, что множество всех доступных в рамках модели катастрофоустойчивых решений $\{DRS\}$ включает подмножество реализованных в КАИС решений $\{DRS'\}$, т. е. $\{DRS\} \subset \{DRS'\}$.

Множество требований, предъявляемых организацией-владельцем КАИС к уровню ее катастрофоустойчивости, представляет собой «эталонные» значения множества показателей оценки катастрофоустойчивости, которые являются входными данными и задаются на этапе сбора информации об исследуемой КАИС. Для описания множества требований организации владельцем используется следующий кортеж:

$\{R_{DRIS}\}=\{L^v, T_R^v, D_{class}^v, N_{Dlost}^v, Z^v, T_{DRS}^v, C_{DRS}^v, R_{isko}^v\}$,

где L^v, T_R^v, D_{class}^v, N_{Dlost}^v, Z^v – показатели катастрофоустойчивости; T_{DRS}^v – приемлемое время развёртывания катастрофоустойчивых решений; C_{DRS}^v – максимальные финансовые затраты на развёртывание катастрофоустойчивых решений; R_{isko}^v – предельно допустимый уровень риска; v – степень важности выполнения каждого требования, описывается множеством базовых значений $v=\{1,2,3\}=\{$низкая важность, средняя важность, высокая важность$\}$.

Множество $\{DF\}$ представляет собой множество дестабилизирующих факторов, аварий и катастроф, порождаемых существенной средой. Каждый элемент из множества $DF_i \in \{DF\}$ описывается вектором $DF_i=(P,U)$, где P – вероятность наступления дестабилизирующего фактора, U – потенциально возможный ущерб.

В соответствии с [5–7] функция принятия решений IMS, реализованная с использованием технологии функционирования искусственных иммунных систем, может быть представлена следующим кортежем:

$IMS=(S_t,\{DF\},\{DRS\},\{R_{DRIS}\}, Sp,\{DET\},\{ANG\},\{ANT\})$,

где $Sp=(L, T_R, D_{class}, N_{Dlost}, Z)$ – вектор текущих значений показателей катастрофоустойчивости исследуемой ИС, выделяется модулем «макрофагом» разработанной ИМС из вектора текущего состояния системы $S_t \in \{S\}$.

$DET=\{det_1, det_2, \ldots, det_m\}$ – набор множества детекторов двух типов мощностью m, отвечающих за решение задач классификации состояний КАИС и выявление потенциально опасных дестабилизирующих факторов, которые участвуют в формировании «иммунной памяти», путем добавления в базу данных информации о результатах проведенной классификации и принятых детекторами решениях. Детекторы первого типа $DET^S \in DET$ представляют собой шаблоны, описывающие «нормальные» состояния системы, реагируют на возможные отклонения значений вектора Sp от «нормальных» значений, описанных в шаблонах, и сообщают об «аномальном» состоянии системы, что указывает на необходимость проведения корректировки текущей катастрофоустойчивости системы путем подбора катастрофоустойчивых решений. Детекторы второго типа $DET^{DF} \in DET$ отвечают за классификацию дестабилизирующих факторов и выявление наиболее критичных из них.

ANG – множество антигенов;

ANT – множество антител.

На вход функции IMS подаются следующие данные (рис. 1): вектор $S_t \in \{S\}$, характеризующий текущее состояние исследуемой КАИС; множество актуальных для исследуемой КАИС дестабилизирующих факторов $\{DF\}$ с заданными значениями вероятности реализации и потенциальным ущербом; множество определенных организацией-владельцем требований $\{R_{DRIS}\}$; множество катастрофоустойчивых решений $\{DRS\}$.

На выходе функции будет информация о принятых решениях и вектор измененного состояния КАИС S_{tnew}.

Основываясь на принципах, изложенных в [6, 8, 9], в структуре разработанной модели иммунной системы можно выделить следующие основные блоки (рис. 2):

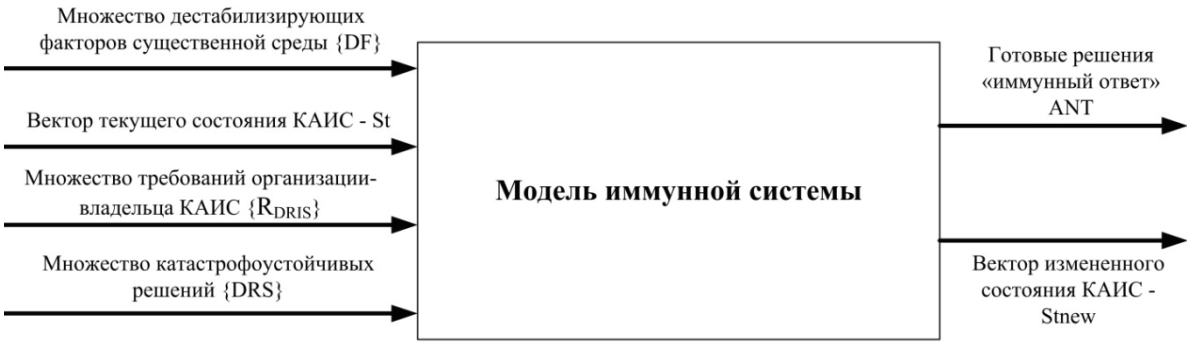

Рис. 1. *Модель искусственной иммунной системы*

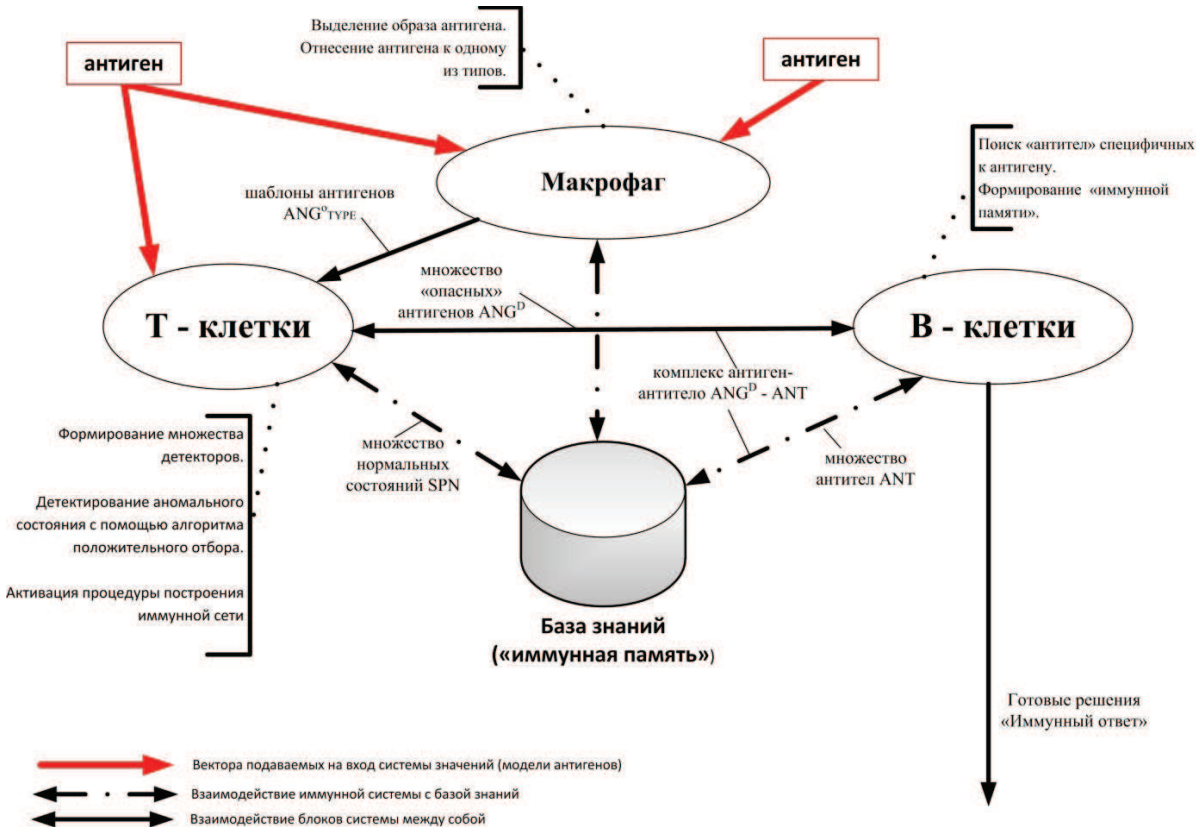

Рис. 2. *Структура иммунной системы принятия решений*

- «макрофаг» отвечает за выделения образов (шаблонов) антигенов из поданных на вход иммунной системы векторов значений и отнесение к одному из двух типов антигенов ANG^{O}_{TYPE};
- «Т-клетки Тимуса» предназначены для идентификации и выявления «аномальных» состояний КАИС;
- «В-клетки», инициирующие запуск процедуры «иммунного ответа», – поиска наиболее эффективных катастрофоустойчивых решений в случае обнаружения «аномальных» состояний системы и выявления потенциальных «антигенов» – наиболее критичных по уровню риска, вероятности реализации и объему потенциального ущерба дестабилизирующих факторов;
- «клетки иммунной памяти», содержащие информацию о ранее принятых системой решениях, правилах классификации и распознавания состояний системы, представляют собой базу знаний ИМС.

Для проведения анализа и оценки катастрофоустойчивости ИС в соответствии с предложенной методикой и формальной моделью автором было разработано алгоритмическое и программное обеспечение системы анализа катастрофоустойчивости ИС, архитектура которой представлена на рис. 3.

На основании собранных данных о технико-эксплуатационных характеристиках анализируемой ИС и требований, предъявляемых организацией-владельцем ИС к показателям катастрофоустойчивости, данная система позволяет [1, 3, 10, 11]:

- рассчитать такие показатели катастрофоустойчивости системы, как уровень катастрофоустойчивости; класс доступности, время восстановления; объем потерянных данных, живучесть системы;
- составить модель дестабилизирующих факторов (множество катастроф различного характера с указанием вероятности реализации и потенциального ущерба по каждому воздействию), потенциально опасных для ИС;
- оценить степень соответствия показателей катастрофоустойчивости системы требованиям организации-владельца;
- составить карту рисков и отобрать наиболее критичные для ИС дестабилизирующие факторы;
- составить различные варианты проектов катастрофоустойчивых решений и найти наиболее эффективный из них.

В соответствии с подходами к построению моделей ИС, предложенными в работах [12–14], при проведении экспериментальных исследований разработанной системы были использованы модели локальных и распределенных ИС. При проведении моделирования были получены следующие данные, представленные в таблице. В таблице приведены значения рассчитанных показателей катастрофоустойчивости ИС с различными технико-эксплуатационными характеристиками до и после применения предложенных разработанной системой проектов катастрофоустойчивых решений.

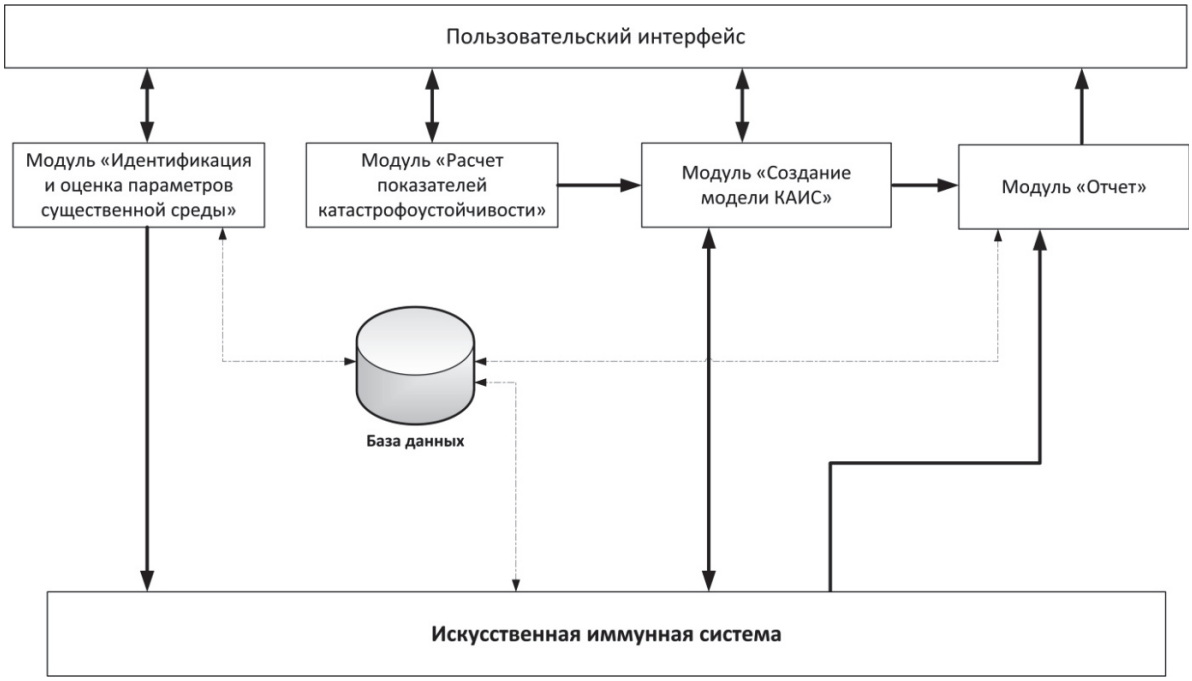

Рис. 3. *Архитектура системы анализа катастрофоустойчивости*

Таблица. *Значение показателей катастрофоустойчивости ИС до и после принятия катастрофоустойчивых решений*

Информационная система						
Тип	на базе локальной сети			распределенного типа		
Показатели катастрофоустойчивости	1	2	3	1	2	3
T_R (до принятия катастрофоустойчивых решений), ч	46	50	25	24	30	8
T_R' (после принятия катастрофоустойчивых решений), ч	32	35	16	16	20	7
L (до принятия катастрофоустойчивых решений)	2	2	3	4	3	5
L (после принятия катастрофоустойчивых решений)	3	3	5	5	4	5
Dclass (до принятия катастрофоустойчивых решений)	1	1	2	4	3	5
Dclass' (после принятия катастрофоустойчивых решений)	1	2	3	4	4	5
Z (до принятия катастрофоустойчивых решений)	0,6	0,58	0,83	0,83	0,86	0,95
Z'(после принятия катастрофоустойчивых решений)	0,75	0,72	0,91	0,91	0,89	0,96

Анализ представленных данных показывает, что применение рекомендованных решений на практике поможет улучшить значения ряда показателей катастрофоустойчивости системы: сократить среднее время восстановления системы на 32 %; повысить средний уровень живучести ИС на 10 %; повысить уровень катастрофоустойчивости системы в 67 % на одну позицию и в 16 % – на две; в 50 % случаях также наблюдается повышение класса доступности системы.

Таким образом, можно сделать вывод о том, что разработанная система анализа катастрофоустойчивости может применяться как на этапе проектирования и разработки катастрофоустойчивых ИС, так и в процессе их эксплуатации в качестве инструмента мониторинга и поддержки принятия решений. Полученные в результате использования системы анализа катастрофоустойчивости данные будут иметь большое значение при разработке плана реализации катастрофоустойчивых решений, пошаговое внедрение и своевременная корректировка которых позволит не только уменьшить потери в случае реализации катастрофы, но и по возможности полностью нейтрализовать ее воздействие.

СПИСОК ЛИТЕРАТУРЫ

1. Аткина В.С. Инновационные подходы в оценке и исследовании катастрофоустойчивости информационных систем // Актуальные вопросы информационной безопасности региона в условиях модернизации общества и внедрения инновационных технологий: Матер. Регион. научно-практ. конф. – Волгоград, 9–10 июня 2011. – Волгоград: Изд-во ВОЛГу, 2011. – С. 168–172.
2. Будзко В.И. Количественные оценки отказоустойчивых и катастрофоустойчивых решений // Вопросы защиты информации. – 2003. – № 2. – С. 19–32.
3. Аткина В.С. Подход к оценке катастрофоустойчивости информационной системы // Информационные технологии, системный анализ и управление: Матер. VIII Всеросс. науч. конф. молодых ученых, аспирантов и студентов. – Таганрог, 2010. – С. 240–243.
4. Atkina V.S. Semantic model of disaster recovery information system // European Science and Technology: international scientific conference. – Wiesbaden, Germany, 2012. – P. 162–164.
5. Гладыш С.В. Иммунокомпьютинг в управлении инцидентами информационной безопасности // Искусственный интеллект. – 2008. – Вып. 1. – С. 123–130.

6. Литвиненко В.И., Бидюк П.И., Фефелов А.А., Баклан И.В. Гибридная иммунная сеть для решения задач структурной идентификации // Нейронные сети. – 2006. – № 9. – С. 143–155.
7. Аткина В.С. Применение иммунной сети для анализа катастрофоустойчивости информационных систем // Известия ЮФУ. Технические науки. Информационная безопасность. – 2011. – № 12. – С. 203–210.
8. Фокин В.А. Статистическое моделирование данных при оценке состояния биологических систем // Известия Томского политехнического университета. – 2007. – Т. 311. – № 5. – С. 132–135.
9. Хаитов Р.М., Игнатьева Г.Л., Сидорович И.Г. Иммунология. – М.: Медицина, 2000. – 432 с.
10. Аткина В.С. Использование программного комплекса для исследования катастрофоустойчивости информационных систем // Вестник Волгоградского государственного университета. Серия 10. Инновационная деятельность. – 2011. – Вып. 5. – С. 14–18.
11. Аткина В.С. Оценка эффективности катастрофоустойчивых решений // Вестник Волгоградского государственного университета. Серия 10. Инновационная деятельность. – 2012. – Вып. 6. – С. 89–93.
12. Погребной В.К. О построении активных моделей распределенных систем реального времени // Известия Томского политехнического университета. – 2008. – Т. 312. – № 5. – С. 78–84.
13. Погребной А.В. Погребной Д.В. Проектирование структуры локальной сети для распределенной вычислительной системы реального времени // Известия Томского политехнического университета. – 2007. – Т. 311. – № 5. – С. 91–96.
14. Вейбер В.В., Кудинов А.В., Марков Н.Г. Задача сбора и передачи технологической информации распределенного промышленного предприятия // Известия Томского политехнического университета. – 2011. – Т. 319. – № 5. – С. 69–74.

Поступила 23.09.2012 г.

УДК 004.931

РАСПОЗНАВАНИЕ СТРУКТУРИРОВАННЫХ СИМВОЛОВ НА ИЗОБРАЖЕНИЯХ С ИСПОЛЬЗОВАНИЕМ ГИСТОГРАММ СРЕДНЕЙ ИНТЕНСИВНОСТИ И СВЕРТОЧНОЙ НЕЙРОННОЙ СЕТИ

А.А. Друки

Томский политехнический университет
E-mail: druki2008@yandex.ru

Разработаны и представлены алгоритм выделения области расположения символов на сложном фоне и алгоритм выделения символов на основе гистограмм средней интенсивности. Для решения задачи распознавания символов разработана и представлена сверточная нейронная сеть.

Ключевые слова:
Обработка изображений, распознавание символов, нейронные сети, гистограммы средней интенсивности.

Key words:
Image processing, character recognition, neural networks, histogram of average intensity.

Введение

Современные технологические, производственные и офисные системы в процессе своего функционирования используют информацию о маркировке объектов. Информация о маркировке грузов, вагонов, контейнеров, автомобильных номерных знаков позволяет рациональным образом организовывать процесс технологической обработки информации, вести учет и контроль изделий, материалов, транспортных средств. В основе процессов использования маркировки (текстово-цифровых меток) лежит технология автоматизированного распознавания структурированных символов. Потребность в такой технологии вызвала необходимость создания методов, моделей и систем распознавания структурированных символов [1].

В настоящее время такие технологии реализуются тремя традиционными методами – структурным, признаковым и шаблонным. Каждый из этих методов ориентирован на свои условия применения, для которых они являются эффективными. Вместе с тем всем этим методам присущи недостатки. Наиболее существенные из них – низкая устойчивость к изменениям масштаба, смещениям, поворотам, смене ракурса и прочим искажениям.

Эти недостатки особенно ярко проявились при масштабной эксплуатации программно-технологических систем, использующих в своей основе эти методы. Практически у всех систем распознавания структурированных символов точностные характеристики резко падают и становятся ниже технологически приемлемых при искажении аффинными и проекционными преобразованиями. Вместе с тем технологические условия получения информации о маркировке не позволяют полностью устранить эти искажения [2].

Анализ методов распознавания структурированных символов показал, что для решения данной задачи эффективно использовать искусственные нейронные сети, в связи с тем, что они являются слабо чувствительными к искажениям входного сигнала, а так же обеспечивают возможность полу-