Serpeninov Oleg Vitalevich
E-mail: serpeninov53@mail.ru.
24/50, M. Nagibin's Avenue, Rostov-on-Don, Russia.
Phone: +79185751114.
The Department of Information Technology and Information Protection; Cand. of Eng. Sc.; Associate Professor.

Samoilin Evgenie Aleksandrovich
Rostov branch of Military Academy of Strategic Rocket Armed Forces Named after Peter-The-Great.
24/50, M. Nagibin's Avenue, Rostov-on-Don, Russia.
Phone: +79085157501.
The Chief of Department; Cand. of Eng. Sc.

УДК 004.056.5, 004.89

В.С. Аткина

ПРИМЕНЕНИЕ ИММУННОЙ СЕТИ ДЛЯ АНАЛИЗА КАТАСТРОФОУСТОЙЧИВОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Целью исследования является предложение нового подхода к анализу катастрофоустойчивости информационных систем, построенного по принципу биоанологии на базе технологии искусственных иммунных систем. Задачи, решаемые в исследовании: обоснование возможности применения искусственных иммунных систем для описания и моделирования катастрофоустойчивых систем; определение принципов функционирования катастрофоустойчивой информационной системы, синтез модели. Результаты исследования: выделены целевые характеристики иммунной системы, разработана и описана модель катастрофоустойчивой информационной системы с применением иммунного подхода. Описан процесс подбора катастрофоустойчивых решений на основе механизма иммунного ответа.

Информационная система; катастрофоустойчивость; катастрофоустойчивые решения; искусственные иммунные системы; иммунный ответ.

V.S. Atkina

APPLICATION OF IMMUNE NETWORK FOR ANALYSIS OF KATASTROFOUSTOJSIVOSTI INFORMATION SYSTEMS

The goal is to propose a new immunologically-inspired approach to analyze the disaster tolerance information system. The problems solved in the study: rationale possibility of using artificial immune systems for the description and simulation of disaster tolerance systems; defining the principles of operation of disaster tolerance information system; synthesis the model. The results of the research are: the focused target properties of immune systems; the model of disaster tolerance information a system is developed and described using the immune approach; described the process selection of disaster recovery solutions based on the mechanism of the immune response.

Information system; disaster tolerance; disaster recovery solutions; artificial immune systems; immune response

Настоящее время характеризуется постоянным возникновением чрезвычайных ситуаций различного рода в самых различных областях человеческой деятельности. Изменение климата, и как следствие стихийные бедствия, имеющие самые различные последствия для всех сфер жизни общества (например, события в Японии 2011 г.), террористическая угроза (особенно после известных событий 11 сентября 2001 г. в

США), техногенные катастрофы, которые, 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 информационных систем (ИС), входящих в состав современных предприятий (в том числе и виртуальных предприятий), является одним из важнейших стратегических направлений развития экономики. Следовательно, актуальным направлением является исследование и решение задач повышения катастрофоустойчивости как бизнес-процессов, так и информационных систем (ИС), обеспечивающих их выполнение.

Сейчас создание катастрофустойчивых ИС (КАИС) обеспечивается за счет применения и использования различных катастрофоустойчивых решений, направленных на обеспечение:

- непрерывности функционирование ИС;
- восстановления функционирования ИС.

Таким образом, решая задачи проектирования, создания и сопровождения КАИС необходимо анализировать структурно-функциональную составляющую системы, а также оценивать эффективность используемых катастрофустойчивых решений, для обеспечения непрерывности бизнес-процессов, своевременной доступности информации, обрабатываемой в КАИС, и ее восстанавливаемости.

Существующие зарубежные и отечественные инструментальные средства обеспечения планирования непрерывности бизнеса (Business Continuity Planning) позволяют использовать универсальные архитектуры баз данных для упрощения процедур анализа риска и развития планов по восстановлению и непрерывности бизнеса, упростить процессы поддержки текущих планов непрерывности бизнеса, синхронизировать и поддерживать актуальную информацию, используя интерфейсы других приложений, корректировать управление компанией с учетом планов непрерывности бизнеса. Вместе с тем они не обеспечивают проведения комплексной автоматизации процессов управления структурной динамикой ИС в целях повышения их безопасности, слабо адаптируются к ситуациям, при которых возможно появление нерасчетных нештатных ситуаций, не ориентированы на упреждающие действия [5]. А это означает, что использование только этих средств не достаточно для проведения анализа и прогнозирования поведения КАИС в условиях воздействия дестабилизирующих факторов. Следовательно, возникает необходимость в разработке методов, моделей и алгоритмов, позволяющих провести структурно-функциональный анализ КАИС, спрогнозировать поведение и состояние системы в условиях дестабилизирующих воздействий, предложить варианты управляющих решений, позволяющих повысить адаптивность КАИС к катастрофическим воздействиям различного рода.

В данной работе для исследования катастрофустойчивости ИС предлагается использовать модель КАИС, в основе которой лежит принцип функционирования иммунной системы человека.

Искусственные иммунные сети – информационные методологии, использующие понятия теоретической иммунологии для решения прикладных задач. Иммунные сети (ИМС) – это адаптивные системы для обработки и анализа данных, которые представляют собой математическую структуру, имитирующую некоторые функции иммунной системы человека и обладающую такими свойствами, как способность к обучению, прогнозированию на основе имеющихся временных рядов и принятию решения в незнакомой ситуации. ИМС не нуждаются в заранее известной модели, а строят ее на основе полученной информации в виде времен-

ных рядов. Данные системы применяются при решении плохо алгоритмизируемых задач, таких как прогнозирование, классификация и управление [1].

В настоящее время в информационной безопасности начинают активно применять технологии искусственных иммунных сетей (ИИМС) для решения таких задач как:

1) обнаружение атак;
2) распознавание новых компьютерных вирусов.

Однако возможности применения ИИМС более широки, в частности в данной работе предлагается использовать этот подход для автоматизации и интеллектуализации процесса анализа катастрофоустойчивости информационных систем. Это является возможным, поскольку между КАИС и системой организма человека (в частности его естественной ИМС) можно провести ряд параллелей:

ИМС постоянно функционирует в организме, отслеживая его состояние и в случае обнаружения дестабилизирующего воздействия, активизируется направляя всю свою деятельность на устранение причины и последствий воздействия. По структуре ИМС представляет собой высокопараллельную распределённую децентрализованную систему временных коллективов клеток (В-, Т-лимфоцитов, макрофагов, фагоцитов, лимфокинов и др.), способную к адаптивной интеллектуальной обработке информации [2]. Она способна: распознавать и делить клетки или молекулы внутри организма на свои и чужие и в зависимости от вида антигена вырабатывать определенные защитные механизмы. При этом результатом распознавания является обучение и формирование памяти к антигену. Знания о схожих антигенах используются при реакции на новые инфекции [2]. Реакция на антиген может происходить не только на уровне отдельных распознающих единиц, но и на общесистемном уровне (в зависимости от уровня серьезности и способа проникновения инфекции [4]). Локальные взаимодействия определяют и реализуют глобальную иммунную реакцию, что в совокупности с непрерывной изменчивостью и адаптивностью иммунной памяти к частоте и силе антигенных сигналов является примером эффективной защиты при ограниченных ресурсах [2].

Исходя из определения, КАИС – это система, способная сохранять критически важные данные и продолжать выполнять свои функции после массового (возможно, целенаправленного) уничтожения своих компонентов в результате различных катаклизмов, как природного характера, так и инспирированных человеком, или в случае нарушения доступности системы за минимальное время восстанавливать свою работоспособность [3], т.е. как и живой организм человека, КАИС обладает определенной живучестью, что позволяет ей противодействовать внешним деструктивным воздействиям, а в случае своего повреждения восстанавливаться за счет определенных ресурсов.

При этом защита и восстанавливаемость КАИС обеспечиваются за счет выработанных и внедренных катастрофоустойчивых решений, которые являются защитным механизмом от воздействия дестабилизирующих факторов.

В зависимости от типа деструктивного воздействия, его направленности и последствий для системы подбираются и формируются группы катастрофоустойчивых решений определенного типа, которые являются наиболее эффективными именно для этой конкретной ситуации.

Таким образом, на основании рассмотренной выше аналогии можно выделить следующие общие принципы функционирования КАИС и ИМС:

1) способность регистрировать, выявлять и определять место деструктивного воздействия на элемент структуры системы;
2) проводить оценку серьезности дестабилизирующих воздействий на ранних стадиях их реализации;

3) идентифицировать тип деструктивного воздействия на основе оперативного анализа и принимать решения в условиях не полной определенности имеющейся информации и при необходимости генерировать сигнала тревоги;
4) вырабатывать защитные механизмы, специфичные к соответствующему деструктивному воздействию;
5) запускать процесс восстановления (регенерации) поврежденных элементов.

Обобщенную модель КАИС можно описать в виде следующего кортежа:

$$ISDRsys = (IR, TR, DF, S, SDR, DRS, DMF, T),$$

где IR – информационные ресурсы;
TR – телекоммуникационные ресурсы;
DF – дестабилизирующие факторы;
S – текущее состояние системы;
SDT – множество устойчивых состояний системы;
DRS – катастрофоустойчивые решения;
DMF – функция принятия решений (реагирования);
T – время.

При этом параметр IS – будет являться входным значением для рассматриваемой системы; DF – непредсказуемые внешние воздействия, катастрофы и угрозы, которые влекут за собой выход системы из состояния равновесия; TR – «операторы преобразования», внутренние процессы, происходящие в системе.

Множество устойчивых состояний системы $SDT=\{SDT_1 \ldots SDT_m\}$ определяет нормальные шаблоны активности КАИС, каждое устойчивое состояние SDT_i характеризуется конечной системой показателей, которые оценивают структуру и различные аспекты функционирования КАИС, а также параметры катастрофоустойчивости, и задаются следующим кортежем, представленным ниже:

$$SDTi = (G_{IS}, L, T_R, T_D, P_{max}, L_{max}, R_l, Z, A, I, T),$$

где G_{IS} – граф, описывающий физическую структуру КАИС;
L – уровень катастрофоустойчивости;
T_R – время восстановления;
T_D – время развертывания катастрофоустойчивых решений;
P_{max} – предельная стоимость внедрения решений;
L_{max} – максимально допустимые финансовые потери;
R_l – уровень надежности;
Z – живучесть системы;
A – требования к доступности информации;
I – требования к целостности информации;
T – требования к актуальности информации.

Текущее состояние системы S характеризует состояние КАИС в данный момент времени, и по аналогии с шаблонами, устойчивых состояний системы, также описывается системой показателей, представленной в виде вектор-функции $\vec{S}=$ $=(G_{IS}, L, T_R, T_D, P_{max}, L_{max}, R_l, Z, A, I, T)$.

По аналогии с основными положениями иммунологии в КАИС имеется некоторое количество уже внедренных катастрофустойчивых решений, которые позволяют системе соответствовать предъявляемым требования к текущей катастрофоустойчивости, т.е. предсуществует ненулевой уровень иммунокомпетентных клеток со своими рецепторами – антителами (катастрофоустойчивыми решениями), специфичными к всевозможным антигенам (дестабилизирующим факторам). Множество катастрофоустойчивых решений представляет собой множество

$$DRS = \{P_д, P_з, P_в P_{из}, P_{п.восст}, P_{цод}, P_{с.х.}, P_к, P_{е.цод}, P_{лс}, P_{влс}\},$$

где $Р_д$ – дамп критических ресурсов;

$Р_з$ – зеркалирование данных;

$Р_в$ – виртуализация серверов;

$Р_{из}$ – аппаратная избыточность;

$Р_{п.восст}$ – программа восстановления при катастрофе;

$Р_{цод}$ – резервный ЦОД;

$Р_{с.х.}$ – система хранения данных;

$Р_к$ – кластерные системы;

$Р_{е.цод}$ – единый вычислиельный центр;

$Р_{лс}$ – резервные линии связи;

$Р_{влс}$ – высокоскоростные линии связи.

Процесс функционирования такой КАИС в условиях воздействия дестабилизирующих факторов с применением иммунного подхода описывается следующим образом. Будем предполагать, что КАИС характеризуется состоянием S, которое известно в любой момент времени T. Кроме того, в процессе функционирования КАИС происходит периодическое сопоставление текущего состояния системы S с состояниями SDT из множества шаблонов, описывающих нормальную активность системы. Любое не совпадение на данном шаге означает изменение в работе системы, что может быть следствием воздействия дестабилизирующих факторов. В качестве функции сравнения состояний системы используется мера сходства. Под мерой сходства будем понимать неотрицательную вещественную функцию $C(S, SDT_i)$, обладающую следующими свойствами:

$0 \le C(S, SDT_i) \le 1$, $C(S, SDT_i), = 1$, если $S=SDT_i$, то $C(S, SDT_i)= C(S, SDT_i)$.

В соответствии с [5] данными свойствами обладает континуум эквивалентных мер, представляемых формулой

$$C(S, SDTi) = \frac{2\mu(S \cap SDTi)}{(1+\lambda)[\mu(S)+\mu(SDTi)] - 2\lambda\mu(S \cap SDTi)},$$

где $-1 \le \lambda < \infty$; $\mu(S)$ – мощность множества признаков, удовлетворяющих S состоянию.

Меры сходства могут использоваться для обработки как качественных, так и количественных признаков.

При этом

$$\mu(S) = \sum_j^{11} Sj,$$
$$\mu(S \cap SDTi) = \sum_j^{11} \min\{S_j, SDTi_j\},$$
$$\mu(S \cup SDTi) = \sum_j^{11} \max\{S_j, SDTi_j\}.$$

Если сравнение структур осуществляется по качественным признакам, то $S_j \in \{0,1\}$, в случае количественных признаков – S_j принимают значения либо в установленной шкале, либо в интервале [0, 1].

Любое воздействие дестабилизирующего фактора на элементы структуры КАИС, влекущее за собой изменение состояния КАИС, воспринимается системой как попадание в организм антигена, в ответ на что формируется «иммунный ответ», заключающийся в подборе наиболее эффективных для данной ситуации защитных механизмов – антител, в качестве которых выступают катастрофоустойчивые решения (рис. 1).

В соответствии с положениями иммунологии, исходя из механизмов, задействованных в реализации иммунного ответа, он может быть различным. В разработанной модели предлагается использовать два типа иммунного ответа:

- неспецифический иммунный ответ;
- специфический иммунитет;

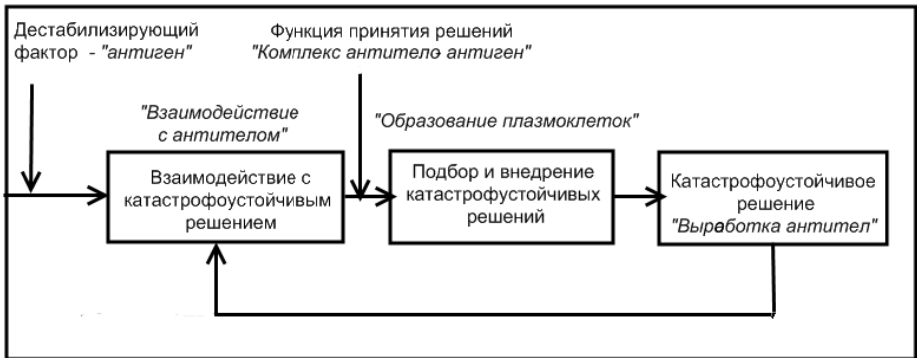

Рис. 1. «Иммунный ответ» КАИС на воздействие дестабилизирующего фактора

Неспецифический иммунный ответ определяется общей живучестью КАИС и выступает, как первый этап борьбы с дестабилизирующим воздействием. Он запускается сразу же после его реализации и заключается в формировании «очага поражения», т.е. локализации места воздействия дестабилизирующего фактора на элементы КАИС с целью предотвращения дальнейшего цепного нарушения процесса функционирования подсистем КАИС и деградации ее структуры. Защитный механизм связан с возможностью реконфигурации системы и включает в себя следующие этапы:

- определение и анализ времени и места отказа ресурса;
- снятие с решения задачи, выполняемой на данном ресурсе;
- передачу задачи на другой ресурс;
- исключение отказавшего ресурса из конфигурации КАИС;
- попытка замены его резервным близкими функциональными возможностями;
- исключение связей с отказавшим ресурсом и запрет на доступ к нему;
- попытка восстановления отказавшего ресурса.

Специфический иммунитет – это вторая фаза защитной реакции организма, его основной характеристикой является распознавание дестабилизирующего воздействия и выработка факторов защиты направленных специально против него.

В разработанной модели КАИС процесс выработки «иммунного ответа» осуществляется посредством функции принятия решений (реагирования) DMF. Функция осуществляет следующие действия:

- детектирование – определение факта и места деструктивного воздействия на элементы КАИС, в основе лежит принцип функционирования макрофагов;
- идентификация дестабилизирующих факторов (антиген), что соответствует поведению клеток Т-хелпперов;
- координация соответствует поведению клеток Т-регуляторов и заключается в подборе катастрофоустойчивого решения для противодействия дестабилизирующему воздействию и последующем анализе эффективности его применения, и подборе нового катастрофоустойчивого решения в случае малой эффективности текущего, сохранение информации о результатах в базу данных для дальнейшего использования, с целью повышения адаптивности системы. При этом наиболее эффективными будут являться те группы решений, которые наиболее быстро минимизируют повреждения КАИС за фиксированное время T:

$$J = \frac{1}{T}\int_0^T \sigma V(t)dt \to min,$$

где σ – скорость поражения структуры КАИС в результате воздействия дестабилизирующих факторов; V(t) – концентрация отказов в структурных элементах «пораженной» части КАИС;

- ♦ реагирование, заключается в применении выбранного катастрофоустойчивого решения, алгоритм действия основан на поведении фагоцитов, имеющих антитела для уничтожения антигена.

Процесс анализа катастрофоустойчивости ИС на примере разработанной модели КАИС будет включать в себя следующие этапы:

1. Сбор информации об КАИС для исследования. На данном этапе осуществляется ввод входных параметров модели, содержащих информацию о структуре и топологии КАИС, ее информационных и телекоммуникационных ресурсах, уже имеющихся катастрофоустойчивых решениях.
2. Обработка информации. На данном этапе осуществляется расчет показателей характеризующих процесс функционирования КАИС, формирование, заполнение и сохранение в базу данных шаблонов нормальной активности системы, описывающих множество всех устойчивых состояний КАИС.
3. Моделирование дестабилизирующих воздействий. На этом шаге осуществляется отбор наиболее вероятных для данной КАИС дестабилизирующих факторов и выбор места их воздействия на элементы структуры КАИС.
4. Анализ результатов моделирования. Данный этап связан с запуском процедуры «иммунного ответа», по результатам которого моделируются возможные сценарии деградации структуры КАИС, происходит оценка тяжести последствий дестабилизирующего воздействия для КАИС и времени его локализации при той или иной группе катастрофоустойчивых решений. Анализируется и сравнивается начальная способность КАИС, противодействовать воздействию дестабилизирующих факторов, с ее способностью после внедрения новой группы решений. Формируется база данных содержащая информацию о типах дестабилизирующего воздействия и наиболее эффективных механизмов защиты от них.
5. Выработка рекомендаций. На основании полученных в результате анализа данных делается вывод о катастрофоустойчивости ИС, возможных рисках и катастрофах, наиболее эффективных решениях и в соответствии с этим формируются рекомендации.

Практическая значимость работы заключается в следующем: предложенные модель и методы анализа КАИС могут использоваться при создании и сопровождении реальных КАИС в качестве методов мониторинга, анализа и прогнозирования ситуаций, разработки вариантов управляющих решений, процедур их выбора и реализации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Самигулина Г.А.* Разработка интеллектуальных экспертных систем прогнозирования и управления на основе искусственных иммунных систем // Теоретическая информатика. – 2009. – Вып. 4. – С 15-22.
2. *Гладыш С.В.* Иммунокомпьютинг в управлении инцидентами информационной безопасности // Искусственный интеллект. – 2008. – Вып. 1. – С. 123-130.
3. *Аткина В.С.* Живучесть системы как показатель ее катастрофоустойчивости // Проблемы обеспечения информационной безопасности в регионе : материалы III Регион. науч.-практ. конф., г. Волгоград, 20 апр. 2010 г. – Волгоград: Изд-во ВолГУ, 2010. – 124 с.
4. *Петров Р.В.* Иммунология. – М.: Медицина, 1987. – 416 с.
5. *Павлов А.Н., Соколов Б.В.* Структурный анализ катастрофоустойчивой информационной системы // Труды СПИИРАН. – 2009. – Вып. 8. – С. 128-153.

Статью рекомендовал к опубликованию д.т.н., профессор О.Б. Макаревич.

Аткина Владлена Сергеевна
Волгоградский государственный университет.
E-mail: atkina.vladlena@yandex.ru.
400062, г. Волгоград, пр. Университетский, 100.
Тел.: 88442460368.
Кафедра информационной безопасности; ассистент.

Atkina Vladlena Sergeevna
Volgograd State University.
E-mail: atkina.vladlena@yandex.ru.
100, Universitetsky Prospect, Volgograd, 400062, Russia.
Phone: +78442460368.
The Department of Information Security; Assistant.

УДК 004.056.5, 004.89

А.Ю. Оладько

МОДЕЛЬ АДАПТИВНОЙ МНОГОАГЕНТНОЙ СИСТЕМЫ ЗАЩИТЫ В ОПЕРАЦИОННОЙ СИСТЕМЕ SOLARIS 10

Целью исследования является предложение нового подхода к защите информационных систем под управлением операционной системы Solaris 10. Предлагается модель адаптивной системы защиты, построенной на базе многоагентного подхода и технологии искусственных иммунных систем. Задачи, решаемые в исследовании: обоснование возможности применения многоагентного подхода и искусственных иммунных систем для описания и моделирования системы защиты от атак, определение принципов функционирования иммунной системы. Результаты исследования: разработана структура модели и описаны функции иммунной многоагентной системы защиты, описаны принципы инициации первичного и вторичного иммунного ответа; проведено сопоставление элементов иммунной системы человека и элементов операционной системы и системы защиты.

Операционная система; многоагентная система; иммунная система; антиген; иммунный ответ; атака.

A.Yu. Oladko

MODEL OF ADAPTIVE MULTI-AGENT PROTECTION SYSTEMS IN THE SOLARIS 10 OPERATING SYSTEM

The goal of research is to propose a new approach to protect of information systems running Solaris 10 operating system. Model is proposed adaptive protection system built on the basis of multi-agent system and the technology of artificial immune systems. The problems solved in the study: rationale possibility of using multi-agent system and artificial immune systems for describing and modeling the system protection from attacks, the definition of the principles of the immune system. The results of the research are: the structure of the model and describes the functions of immune multi-agent protection system; principles of the initiation of primary and secondary immune response are described; comparison of the elements of the human immune system and elements of the operating system and security are held.

Operating system; multi-agent system; the immune system; antigen; immune response; attack.

Sun Solaris представляет собой мощную и гибкую операционную систему, существующую в вариантах как для процессоров SPARC, так и x86. Solaris предназначается для работы в корпоративных вычислительных сетях и обеспечивает чрезвычайно эффективный и надежный доступ к системам в целом, серверам, базам данных, принтерам и другим сетевым ресурсам.