данных и информации. Однако и традиционные решения точно так же уязвимы, поскольку их работа неизбежно связана с проблемами в сфере коммуникаций, риском выхода из строя оборудования и человеческим фактором. Следует четко понимать особенности реализации поддержки бизнес-процессов с помощью «облачных» технологий, оценивая критические риски для каждого конкретного решения. То же самое относится и к попыткам интеграции разных облачных сервисов.

Литература

1. Журнал «Открытые системы» от 06.2010.
2. Электронная энциклопедия Wikipedia [Электронный ресурс]: http://www.wikipedia.org .
3. Безопасность в облаках // Интернет-журнал ibusiness [Электронный ресурс]: http://www.ibusiness.ru/15656 .
4. Проблемы облачных вычислений // Интернет-журнал Computerra [Электронный ресурс]: http://www.computerra.ru/vision/485315/ .
5. Журнал «Хакер».
6. http://technet.microsoft.com/ru-ru/magazine/gg607453.aspx .
7. http://winsecurity.ru/articles/microsoft-azure-security-cloud.html .
8. http://habrahabr.ru/blogs/cloud_computing/112961/ .
9. http://www.ci.ru // Статьи Игоря Козлова.

Нестерук Л.Г., Нестерук Ф.Г.

Об организации распределенных средств интеллектуальной защиты информации

(СПбГУЭФ, Санкт-Петербург)

Актуальность обсуждаемой тематики заключается в том, что перспективные разработки средств защиты информации (СЗИ) должны быть сориентированы на аналогию с механизмами защиты (МЗ) биосистем. При этом МЗ должны соответствовать адаптационным свойствам биологических систем, подтвердивших свою жизнеспособность в течение длительного процесса эволюции [1–5]. Известно, что в зависимости от реализуемых механизмов обеспечения безопасности как реакцию биосистемы на внешние воздействия можно выделить два интеллектуальных уровня: иммунной системы и нервной системы [5–7], аналоги которых целесообразно реализовать в рамках информационно-коммуникационных сетей (ИКС) в условиях высокой динамики угроз, изменения тактики и стратегии проведения компьютерных атак [8].

Анализ текущей обстановки в области моделирования средств иммунной защиты.

Имунная система способна эффективно обрабатывать значительные объемы данных путем высокопараллельных распределенных вычислений [14].

Согласно [15] естественная иммунная система (ЕИС) функционирует как «второй мозг», способна сохранять информацию о предыдущих контактах с антигенами (АГ) и отвечать на ранее не встречавшиеся АГ. Для обработки информации перспективны следующие свойства ЕИС.

- *Распознавание*. ЕИС способна классифицировать белковые структуры: распознавание своего и чужого (одна из основных задач ЕИС).
- *Выделение особенностей.* Макрофаги и другие антиген-представляющие клетки (АПК) выделяют особенности антигенного окружения и выставляют на своей поверхности пептиды АГ для лимфоцитов [16].
- *Разнообразие*. ЕИС использует механизм генерации рецепторов лимфоцитов, гарантирующий взаимодействие лимфоцита с любым неизвестным АГ.
- *Обучение*. ЕИС оценивает структуру АГ через его случайные контакты с клетками ЕИС. Обучение выражено в изменении концентрации лимфоцитов при первичном ответе за счет механизма размножения и супрессии клонов [17].
- *Память*. Часть лимфоцитов в процессе иммунного ответа становится клетками памяти, принимая модифицированную форму и сохраняя информацию о контактах с АГ.
- *Распределенный поиск*. ЕИС – распределенная система, клетки которой многократно циркулируют через кровь, лимфу, органы и ткани, где встречаются с АГ.
- *Саморегуляция*. Иммунная защита обладает свойством саморегуляции и распределённого управления – не существует центрального органа, управляющего функциями ЕИС.
- *Пороговый механизм*. Иммунный ответ и размножение иммунокомпетентных клеток происходят по преодолению некоторого порога концентрации.
- *Совместная стимуляция*. Активация В-лимфоцитов регулируется посредством стимулирующего сигнала от хелперных Т- лимфоцитов. (Т- и В-лимфоциты – основной тип клеток, участвующих в иммунном ответе и обладающих свойствами специфичности, разнообразия, памяти и адаптивности).
- *Динамическая защита.* Клональное размножение и соматическое гипермутирование продуцирует иммунокомпетентные клетки, что позволяет установить динамический баланс между изучающей и защитной функцией адаптивного иммунитета.
- *Вероятностное обнаружение.* Реакции при иммунном ответе представляют стохастический процесс, т.е. лимфоцит взаимодействует со множеством сходных АГ.

В иммунном ответе на АГ важную роль играют такие характеристики, как адаптируемость, специфичность, самотолерантность и дифференцировка.

Модели процессов иммунной системы

Для иммунных механизмов разработаны ряд трактовок, теорий [18, 19], математических моделей [20, 21], включая модели для имитации динамики отдельных компонентов и ЕИС в целом [22, 23] в виде систем дифференци-

альных [20] и стохастических [24] уравнений, клеточно-автоматные модели [25, 26], модели пространства конфигураций [27, 28] и другие.

Модели иммунной системы

Известна теория [29,18], согласно которой ЕИС – адаптивная идиотипическая сеть молекул и клеток, распознающих друг друга даже при отсутствии АГ, в которой динамика концентрации клонов лимфоцитов и молекул иммуноглобулинов описывается системой дифференциальных уравнений. Теория идиотипической регуляции основана на предположении, что клоны лимфоцитов не изолированы, а поддерживают связь путем взаимодействий между своими рецепторами и АТ. Распознавание АГ на системном уровне клонами лимфоцитов осуществляется на основе реакций антиген-антитело. Постулат теории – отдельная клетка продуцирует лишь один тип антител (АТ). Используют формальные и функциональные сети: первые служат для изучения качественной стороны теории, вторые – количественной.

В [20] предложена вероятностная модель идиотипических сетей, предназначенная для описания фазовых переходов. Плоскость фазовых переменных системы уравнений разделяют на докритическую область, область перехода и посткритическую область. Как теория искусственных иммунных систем (ИИС) [18] [20, 30, 22], так и математическое моделирование [31, 32, 33] активно развиваются.

Постановка задачи реализации распределенных средств интеллектуального анализа информации (ИАИ) в составе системы защиты носит комплексный характер и использует биосистемную аналогию, начиная с формы представления информации, информационных процессов программирования и заканчивая архитектурой ИКС со встроенными механизмами обеспечения безопасности [5, 6]. Известно, что биосистемы обладают многоуровневой иерархической системой жизнеобеспечения, реализованной с использованием комплекса механизмов информационной избыточности, защиты и иммунитета [3, 9].

Цель статьи – рассмотрение принципов организации распределенных средств интеллектуального анализа информации в составе двухуровневой иерархической СЗИ, ориентированных на биосистемную аналогию и динамику процессов взаимодействия потоков данных и структур [5, 10].

Двухуровневая иерархическая архитектура адаптивной защиты ИКС включает: нижний интеллектуальный уровень иммунной защиты и верхний адаптивный уровень нейросетевой защиты.

Уровень иммунной защиты ИКС, по аналогии с естественной иммунной системой (ЕИС), должен обладать распределенным характером механизмов защиты, автоматизмом функционирования, децентрализацией управления, то есть внутренним распределенным интеллектом. Согласно [2, 3], ЕИС состоит из центральной и периферической частей:

- центры – производители В- и Т-клеток (костный мозг и тимус);
- основные функции защиты – вне центров – в лимфоидной ткани в виде распределенных по системе мобильных объектов (лимфоциты, антигенпредставляющие и др. клетки);

- мобильные объекты выполняют функцию классификации «свой – чужой»;
- мобильные объекты постоянно мутируют. Образуют клоны клеток-мутантов;
- в среде мутантов целевая функция отслеживается – соответствие «антитело-антиген» («АТ-АГ») согласно принципу комплементарности;
- соответствие «АТ-АГ» – нечеткое, характеризуется степенью принадлежности: сильное соответствие – удачный мутант, слабое – неудачный мутант;
- механизм клонирования удачных мутантов постоянно работает, создавая популяцию удачных мутантов;
- популяции удачных мутантов, содержат клоны с разным уровнем соответствия «АТ-АГ»;
- постоянно работает механизм уничтожения неудачных мутантов;
- запуск механизмов клонирования и уничтожения– пороговый (по концентрации объектов: АГ и АТ);
- реализованы механизмы поддержки (хэлперные клетки) удачных мутантов (при развертывании иммунного ответа) (высокая концентрация АГ), и при свертывании иммунного ответа – подавления (супрессии) (малая концентрация АГ);
- иммунная память постоянно пополняется – актуальная база данных (БД) удачных мутантов поддерживается, в виде В- и Т-клеток памяти;
- осуществляется размещение клеток памяти согласно механизму хоминга (по месту выявления антигена в системе).

Уровень нейросетевой защиты ИКС по аналогии с естественной нервной системой (ЕНС) характеризуется централизованным управлением (головной мозг), распределенными по организму механизмами защиты и обработки информации в виде информационных полей нейронных сетей (НС). ЕНС состоит из центральной и периферической частей [3, 9].

ЕНС – адаптивный инструмент взаимодействия со средой, необходима для формирования рефлексов в ответ на воздействия [9]. Поведенческие реакции в биосистеме – качество нервной системы, свидетельствующее о развитии связи между воздействиями и реакцией организма. Отмечают разделение информации между носителями различной природы: дезоксирибонуклеиновую кислоты (ДНК) и нейронами. Поведенческая информация формируется на основе механизмов, передаваемых через ДНК, а фиксируется в информационном поле ЕНС. Биосистемам свойственно накопление жизненного опыта. Затем передача его потомкам через обучение [9]. Целенаправленность поведения биосистемы развивает форму памяти в виде адаптивных информационных полей НС нервной системы. Уровень нейросетевой защиты ИКС должен реализовать функции распределенной обработки:

- сохранение знаний в информационных полях НС;
- базы отражение знаний (БЗ) на структуру НС;
- БЗ адаптация путем обучения информационных полей НС;

- извлечение знаний путем анализа информационных полей НС после их обучения;
- грубая классификация (наличие / отсутствие угрозы);
- в случае наличия угрозы – классификация детальная по типу угрозы;
- согласно типу угрозы определение в системе места вероятного проявления угрозы с целью ее нейтрализации конкретными механизмами защиты.

Взаимосвязь иммунного и нейросетевого уровней защиты – через системную информацию (ДНК). ДНК – основа «своей» информации для иммунного уровня (выполнение функции классификации «свой-чужой»). ДНК хранит принципы организации и возможность механизмов защиты запуска как иммунного, так и нейросетевого уровня.

Взаимосвязь уровней защиты также должна осуществляться через промежуточные параметры, которые изменяются в результате работы иммунного уровня и могут оцениваться средствами нейросетевого уровня (интеллектуальный анализ, установление логической взаимосвязи параметров).

Иммунная защита в ИКС реализуется в среде передачи сообщений, которая играет роль лимфоидной ткани ЕИС и распределена по узлам сети, выполняющих функции фолликул периферических лимфоидных органов ЕИС.

Как известно, в ЕИС основные события иммунного ответа происходят в фолликулах лимфоидных органов (местах сосредоточения В-клеток). В фолликулах при воздействии антигена формируются центры размножения. В-лимфоциты, стимулированные АГ, интенсивно делятся, и в V-генах (рецепторах) лимфоцитов на несколько порядков повышается частота мутаций. Если мутации приводят к ослаблению сродства рецептора к антигену, клоны гибнут. Наоборот, в случае повышения сродства рецептора к АГ клоны выживают, получают преимущества в размножении и секретируют антитела [3].

Узловые компоненты ИКС, помимо основных сетевых функций, также должны реализовать функции классификации «свой – чужой» (по фрагменту передаваемого пакета сообщений).

К узловым компоненты ИКС коммуникационные средства относят, соответствующие различным уровням эталонной модели открытых систем [11]: повторители – сигнала усиление и разветвление для сегмента компьютерной сети увеличения; мосты и коммутаторы – сети разбиение на сегменты и небольших локальных сетей объединение; маршрутизаторы – к глобальной сети подключение, локальных сетей и их больших частей объединения; шлюзы – функции маршрутизации и объединения сетей с несовместимыми протоколам информационного взаимодействия.

Согласно биоаналогии каждая ИКС может иметь индивидуальное представление пакетов сообщений, используя [5, 6]:

- парафазное кодирование (равное число 0 и 1 в сообщении обеспечивает – аналог равномерного «массы» распределения по молекуле ДНК);
- комплементарное представление информации в виде взаимодополняющих фрагментов (аналог A=T и C≡G связей в молекуле ДНК, здесь A – аденин, G – гуанин, C – цитозин и T – тимин);

- индивидуальное для данной сети чередование взаимодополняющих фрагментов (каждый пакет – контейнер для сообщения и в то же время само сообщение по аналогии с молекулой ДНК).

Каждый пакет может кодироваться в порту передачи сетевого узла и декодироваться в порту приема другого сетевого узла. Пакеты с «чужим» кодированием изымаются из трафика. Способ кодирования – декодирования внутри сети может динамически изменяться (сеансовая перенастройка узлов сети).

Нейросетевая защита ИКС реализуется как специализированная подсистема для целей защиты информации. Архитектура нейросетевой защиты представляется иерархической двухуровневой адаптивной моделью (содержащей адаптивные средства классификации (АСК) на каждом из иерархических уровней СЗИ) [5, 12]:

- нижний уровень классификации – угроз по признакам атаки;
- верхний уровень классификации – места реализации атаки в системе, а именно: указание конкретных уровней СЗИ и механизмов защиты (МЗ) для ее нейтрализации;
- оба уровня – адаптивные, причем первый может быть интеллектуальным (самостоятельно принимающим решения и самостоятельно перестраивающий себя), второй – управляться администратором сети.

В модели адаптивной СЗИ методика оценки защищенности ИКС координирует взаимосвязь АСК угроз и АСК механизмов защиты в виде НС, нечетких НС, систем правил логического вывода. В АСК могут быть использовать самоорганизующиеся НС, например, Adaptive Resonance Theory (ART), ARTMAP или EMANN [2, 13]. Информация в адаптивной СЗИ хранится и может наследоваться в виде распределенных адаптивных информационных полей НС: поля известных угроз на нижнем уровне защиты и поля опыта эксплуатации на верхнем уровне защиты.

Нижний уровень решает задачу классификации угроз по признакам атак, а верхний – задачу классификации МЗ по вектору угроз. Системы правил логического вывода отображаются в топологии нечетких НС для обучения и анализа результатов процесса адаптации.

АСК каждого из уровней СЗИ организованы по иерархической схеме: матрица экспертных оценок ↔ система правил логического вывода ↔ нечеткая НС ↔ самообучающаяся НС. Самообучающаяся НС необходима для решения задачи кластеризации. В процессе самообучения НС добиваются разбиения векторов обучающей выборки на группы, число которых равно числу правил в базе знаний. Обучение нечеткой НС и последующий анализ весов связей вновь введенных формальных нейронов (ФН) позволяет сформировать спецификацию на отсутствующие в СЗИ механизмы защиты и откорректировать матрицу экспертных оценок [8].

В процессе работы СЗИ происходит накопление опыта эксплуатации ИКС, за счет базы знаний (БЗ), параметров нечетких НС, матриц экспертных оценок адаптации. Коррекция матриц экспертных оценок изменяет значения

показателей защищенности ИКС, что отслеживать динамику защищенности и позволяет принимать решение о необходимости модификации СЗИ.

Для обучения/тестирования АСК может быть использован иммунный механизм поиска «чужого» на уровне нейросетевой защиты. Случайно (эволюционным алгоритмом) генерируются векторы (признаков атаки, угроз), которые классифицируются посредством АСК как «свой-чужой». Здесь «свой» известный тип вектора, работе с которым обучена СЗИ, «чужой» – неизвестный для СЗИ тип вектора. Классификация вектора как «чужого» говорит о формировании потенциально опасного вектора, который может поступить в последствии на входы СЗИ. Таким образом может быть сформирована БД потенциально опасных векторов, необходимых для выявления реального «чужого» в ИКС. В системе может быть создан отдельный классификатор, уже обученный на распознавание потенциально опасных векторов.

Организация интеллектуальной нейросетевой защиты. Согласно [10] информационная база (ИБ) состоит из взаимосвязанных базы данных, базы знания и средств ее разработки и управления, а информационные процессы рассматриваются как субъект-объектное взаимодействие. Для субъект-объектного взаимодействия организации требуются две ИБ, которые образуют интеллектуальную базу [10]. Одна информационная база представляет жизненный опыт («память»), а другая – «текущее состояние» системы. В процессе взаимодействия информационных баз возникают новые знания.

Понятие интеллектуальной базы может быть применима к модели адаптивной защиты, которая представлена двухуровневой иерархической структурой [8, 12]:

- нижний уровень – автоматический за счет наличия интеллектуальной базы, которая самостоятельно набирает жизненный опыт в процессе «общения» через коммуникационную среду: одна информационная база представляет жизненный опыт («память»), а другая – «текущее состояние» СЗИ;
- верхний уровень ориентирован на получение информации о динамике изменения нижнего уровня и интеллектуальным не является, т.к. решение принимает администратор сети. Однако уровень содержит БЗ, БД и средства формирования/корректировки логических связей.

При сохранении двухуровневой иерархии назначение и функции уровней СЗИ разные:

- нижний становится интеллектуальным (аналог иммунных механизмов в организме, которые работают оперативно и автоматически, практически без центральной коррекции со стороны нервной системы организма);
- верхний соответствует процессам запоминания в центральной нервной системе, которая может работать значительно медленнее и накапливать опыт под контролем и при участии администратора безопасности.

В момент создания интеллектуального уровня в него с верхнего уровня иерархии (этап наследования) загружают исходные БД и БЗ, как и начальные методы их взаимодействия с внешней средой.

Нижний уровень, в результате информационного обмена (с Интернетом, коммуникационной средой ИКС) автоматически изменяется (постоянно реализуемый этап развития). Причем в процессе работы интеллектуального уровня в ИБ «Текущее состояние», изменяются как исходные БД и БЗ, так и методы их взаимодействия с внешней средой и их собственной коррекции (постоянно выполняемый этап развития – адаптация к внешним условиям, реализуется основное свойство – пластичности). В результате взаимодействия информационной базы «Текущее состояние» и целевых установок верхнего уровня (администратор безопасности) в памяти фиксируются только существенные изменения, реализуется основное свойство стабильности.

Верхний иерархический уровень СЗИ получает с нижнего уровня иерархии системы защиты как динамику состояний как «памяти» (стабильность), так и «текущего состояния» (пластичность) с целью интеллектуального анализа (посредством АСК) и структурной коррекции модели СИБ (посредством методики оптимизации при участии естественного интеллекта администратора безопасности ИКС).

Для организации внешней информационной связи со средой необходимы посредники – параметры физической среды, через которые можно судить о динамике воздействия информационного обмена ИКС с Интернетом. В качестве параметров могут выступать:

- статистика ИКС (частота посещения ИКС, сетевых адресов анализ и пр.);
- статистика операционной системы (открытие, закрытие файлов, операции над файлами, временные параметры, попытки обращения к системным файлам и защищаемым областям памяти и пр.).

Эксперименты. Проведены исследования с целью определения нейросетевой архитектуры, соответствующей задаче классификации / кластеризации для СЗИ.

Типичным представителем НС является многослойный персептрон, недостаток которого состоит в низкой скорости обучения. Это ограничивает возможность оперативной адаптации НС в темпе поступления каждого нового входного вектора. Требуется многократное обучение на всем наборе обучающей выборки. Использованы быстрые алгоритмы обучения многослойного персептрона. Затем происходит «катастрофическое забывание» [35].

НС для визуализации многомерных данных, например самоорганизующиеся карты (COM)(Self-organizing map – ((SOM)) Кохонена [36], обучаются без учителя. Решение задачи кластеризации многомерных векторов не в полной мере удовлетворяет поставленной задаче. Т.к. в зависимости от порядка поступления векторов обучающей выборки будет изменяться местоположение классов на выходной карте.

НС встречного распространения быстро обучаются. Они полезны для моделирования интеллектуальных СЗИ, где важна оперативная начальная

аппроксимация [37], т.е. на этапе первоначального моделирования, а затем подлежат замене на НС, которые могут обеспечить более высокую точность.

НС семейства ART предназначены для классификации многомерных векторов. Способны обучаться инкрементно, с высокой точностью. Обучение происходит за один проход без эффекта «катастрофического забывания», что позволяет отдать предпочтение данному типу НС для решения поставленной задачи.

РАЗРАБОТКА ПРОГРАММНОГО МОДУЛЯ ДЛЯ ИССЛЕДОВАНИЯ ART-СЕТЕЙ [34]

Для нейросетевой архитектуры семейства ART для целей АСК в Microsoft Visual Studio был создан программный модуль (FANNC Test) для исследования сетей Fuzzy ARTMAP и FANNC (рис. 1) по тесту «круг в квадрате».

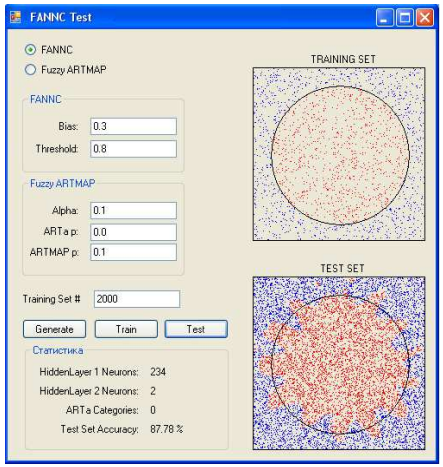
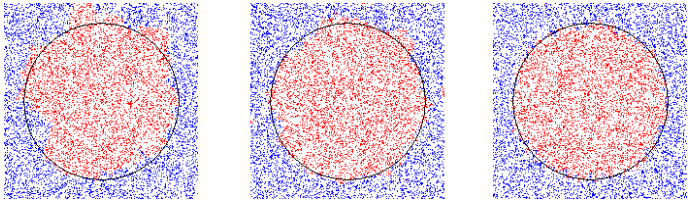


Рис. 1. Программный модуль тестирования ART-сетей

Площадь круга равна площади квадрата. Точки внутри круга принадлежат одному классу, а точки вне круга, но внутри квадрата – другому. Тест позволяет определить точность решения задачи классификации точек, лежащих внутри и вне круга [38].

ИССЛЕДОВАНИЕ ART-СЕТЕЙ ПРИ ОБУЧЕНИИ ДВУМ КЛАССАМ

Проведено исследование способности НС решать задачу классификации в зависимости от параметров, алгоритмов и количества обучающих примеров. Обучающие примеры охватывали в равной степени оба класса. Результаты тестирования в зависимости от числа обучающих примеров для FANNC (рис. 2) и для Fuzzy ARTMAP (рис. 3) приводят к следующим выводам:

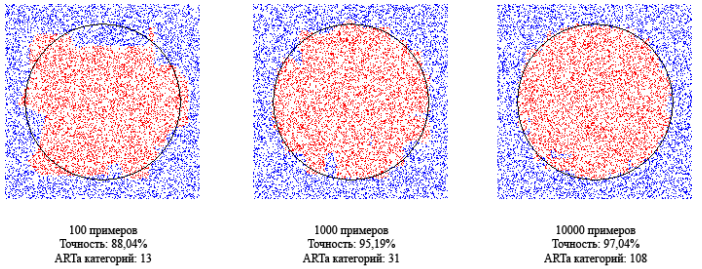


100 examples
Precision:90.94%
NN in 2nd layer:29
NN in 3rd layer:2

1000 examples
Precision:94.92%
NN in 2nd layer:128
NN in 3rd layer:2

10000 examples
Precision:96.09%
NN in 2nd layer:515
NN in 3rd layer:2

Рис. 2. Результаты тестирования FANNC в зависимости от числа примеров



100 examples
Precision:88.04%
ARTa categories: 13

1000 examples
Precision:95.19%
ARTa categories: 31

10000 examples
Precision:97.04%
ARTa categories: 108

Рис. 3. Результаты тестирования Fuzzy ARTMAP
в зависимости от числа примеров

- FANNC обладает лучшей обобщающей способностью при небольшом числе обучающих примеров;
- число ФН во втором слое FANNC при увеличении числа обучающих примеров быстро растет. В результате производительность НС падает;
- при увеличении числа обучающих примеров Fuzzy ARTMAP обладает большей точностью обобщения, чем сеть FANNC;
- с ростом числа обучающих примеров число категорий в модуле ART_a Fuzzy ARTMAP растет не так быстро, как число ФН второго слоя в FANNC.

Дополнительно было проведено исследование зависимости точности FANNC от параметра смещения нейронов в скрытых слоях НС для 100 обучающих примеров и 1000 обучающих примеров. Т.к. результаты классификации FANNC зависели от выбора параметров алгоритма – параметры FANNC приходилось регулярно изменять для поддержания высокой точно-

сти при увеличении числа обучающих примеров. В то время как параметры Fuzzy ARTMAP оставались постоянными.

Заключение. Представлены принципы организации распределенных средств интеллектуального анализа информации в составе системы адаптивной защиты ИКС, ориентированные на биосистемную аналогию.

Актуальна разработка адаптивных средств классификации в составе иерархической модели системы защиты информации и методик оптимизации их структуры путем отслеживания динамики внешней среды. Также моделирование процессов накопления опыта, исходя из результатов интеллектуального анализа информации.

Показана возможность реализации интеллектуального уровня в составе адаптивной СЗИ, решающего задачи самоорганизации и самообучения в процессе информационного обмена с внешней средой.

Литература

1. Darwin C. On the Origin of Species by Means of Natural Selection, or the Preservation of Favoured Races in the Struggle for Life/1859. – P. 502.
2. Искусственные иммунные системы и их применение / Под ред. Д. Дасгупты: Пер. с англ. под ред. А.А. Романюхи. – М.: ФИЗМАТЛИТ, 2006. – 344 с.
3. Хаитов Р.М. Физиология иммунной системы. – М.: ВИНИТИ РАН, 2001. – 224 с.
4. Котенко И.В., Степашкин М.В. Интеллектуальная система моделирования атак на web-сервер для анализа уязвимостей компьютерных систем // Сб. докл. VI Международной конф. по мягким вычислениям и измерениям SCM'2003. – СПб.: СПГЭТУ, 2003. Т. 1. – С. 298-301.
5. Нестерук Ф.Г., Суханов А.В., Нестерук Л.Г., Нестерук Г.Ф. Адаптивные средства обеспечения безопасности информационных систем / Под ред. Л.Г. Осовецкого. – СПб.: Изд-во Политехнического университета, 2008. – 626 с.
6. Нестерук Г.Ф., Осовецкий Л.Г., Харченко А.Ф. Информационная безопасность и интеллектуальные средства защиты информационных ресурсов (Иммунология систем информационных технологий). – СПб.: Изд-во СПбГУЭФ, 2003. – 364 с.
7. Нестерук Г.Ф., Молдовян А.А., Нестерук Ф.Г., Костин А.А., Воскресенский С.И. Организация иерархической защиты информации на основе интеллектуальных средств нейро-нечеткой классификации // Вопросы защиты информации. – 2005. – № 3. – С. 16-26.
8. Kotenko I., Ulanov A. Simulation of Internet DDoS Attacks and Defense. 9th Information Security Conference. ISC 2006. Samos, Greece. August 30 – September 2, 2006. Proceedings. Lecture Notes in Computer Science. Vol. 4176, 2006. – P. 327-342.
9. Мелик-Гайназян И.В. Информационные процессы и реальность. – М.: Наука, 1998. – 108 с.
10. Лачинов В.М., Поляков А.О. Информодинамика или Путь к Миру открытых систем. Изд. 2-е, перераб. и доп. – СПб.: Изд-во СПбГТУ, 1999.

11. Зима В.М., Молдовян А.А., Молдовян Н.А. Безопасность глобальных сетевых технологий. – СПб.: БХВ-Петербург, 2003. – 368 с.
12. Нестерук Г.Ф., Молдовян А.А., Осовецкий Л.Г., Нестерук Ф.Г., Фархутдинов Р.Ш. К разработке модели адаптивной защиты информации // Вопросы защиты информации. – 2005. – № 3. – С. 11-16.
13. Granger E., Rubin M. A., Grossberg S., Lavoie P. Classification of Incomplete Data Using the Fuzzy ARTMAP Neural Network // Proc. Int'l Joint Conference on Neural Networks, vol. IV, 2000. – P. 35-40.
14. Frank S.A. The design of natural and artificial adaptive systems. – N.Y.: Academic Press, M.R.Rose and G.V. Lauder edition, 1996.
15. Rome G.W. The theoretical models in biology. Oxford University Press, 1st edition, 1994.
16. Cohen I. R. The cognitive paradigm and the immunological homunculus // Immunol. Today. 1992. V. 13, № 12. – P. 490-494.
17. Bersini Я, Varela F.J. The immune recruitment mechanism: A selective evolutionary strategy // In: Proc. of the fourth international conference on genetic algorithms, San Diego, July 13-16, 1991. – P. 520-526.
18. Jerne N. K. Towards a network theory of the immune system // Ann. Immunol. (Inst. Pasteur). 1974. V. 125C. – P. 373-389.
19. Mohler R.R., Bruni C, Gandolfi A. A system approach to immunology // Proc. IEEE. 1980. V. 68, № 8. – P. 964-990.
20. Perelson A. S. Immune network theory // Immunol. Rev. 1989. V. 10. – P. 5-36.
21. Varela F.J., Stewart J. Dynamics of a class of immune networks I. Global stability of idiotype interactions // J. Theor. Biol. 1990. V. 144, № 1. – P. 93-101.
22. Vertosick F. T., Kelly R. H. Immune network theory: a role for parallel distributed processing? // Immunology. 1989. V. 66. – P. 1-7.
23. Weinand R. G. Somatic mutation, affinity maturation and antibody repertoire: A computer model // J. Theor. Biol. 1990. V. 143, № 3. – P. 343-382.
24. Chowdhury D., Stauffer D. Statistical physics of immune networks // Physica A. 1992. V. 186. – P. 61-81.
25. Celada F., Seiden P.E. A computer model of cellular interactions in the immune system // Immunol. Today. 1992. V. 13, № 2. – P. 56-62.
26. Santos R.M.Z., Bernardes A. T. The stable-chaotic transition on cellular automata used to model the immune repertoire // Physica A. 1995. V. 219. – P. 1-12.
27. Weisbuch G. A shape space approach to the dynamics of the immune system // J. Theor. Biol. 1990. V. 143, № 4. – P. 507-522.
28. Ishida Y. Fully distributed diagnosis by PDP learning algorithm: Towards immune network PDP model, I, June 17-21, 1990. – P. 777-782.
29. Jerne N. K. The immune system // Sci. Am. 1973. V. 229, № 1. – P. 52-60.
30. Varela F.J., Stewart J. Dynamics of a class of immune networks I. Global stability of idiotype interactions // J. Theor. Biol. 1990. V. 144, № 1. – P. 93-101.
31. Hunt J.E., Cooke D.E. An adaptive, distributed learning system, based on the immune system // In: Proc. of the IEEE international conference on systems, man and cybernetics, 1995. – P. 2494-2499.

32. Ishida Y., Mizessyn F. Learning algorithms on an immune network model: application to sensor diagnosis // In: Proc. of international joint conference on neural networks, China, November 3-6, 1992. V. 1. – P. 33-38.

33. Ishiguro A, Watanabe Y., Uchikawa Y. Fault diagnosis of plant systems using immune networks // In: Proc. of the 1994 IEEE international conference on multisensor fusion and integration for intelligent systems (MFI'94), Las Vegas, October 2-5, 1994. – P. 34-42.

34. Нестерук Ф.Г., Баранюк Т.Н., Нестерук Л.Г., Марченко А.А., Нестерук Г.Ф. Комплементарное кодирование информации в нейросетевых средствах систем защиты информации // Вопросы защиты информации. – 2007. – № 4. – С. 53-57.

35. Carpenter G.A., Milenova B.L. Distributed ARTMAP // Proc. of the International Joint Conference on Neural Networks. 1999.

36. Kohonen T. The self-organizing map // Proceedings of the IEEE, 78, 1990. – P. 1464-1480.

37. Уоссермен Ф. Нейрокомпьютерная техника: Теория и практика. – М.: Мир, 1992.

38. Zhou Z., Chen S., Chen Z. FANNC: A Fast Adaptive Neural Network Classifier // Knowledge and Information Systems. – 2000. – P. 115-129.

Завьялов А.А.

Методология создания корпоративных сервисов и приложений под управлением бизнеса

(СПбГУЭФ, Санкт-Петербург)

Введение

Компаниям в современных условиях приходится мириться с темпом изменения конъюнктуры рынка, изменяя свой бизнес под изменения конкурентного рыночного спроса. Примерно 80 процентов ИТ бюджета компаний тратится на настройку и на расширение существующих приложений. Эти приложения не создаются с задумкой быть гибкими и поэтому, пока бизнес переключается с некоторой задержкой к новым или расширенным процессам, база ИТ не способна справиться с основными изменениями. Традиционные приложения и архитектуры не способны быть на одной волне с бизнес инновациями в основном потому, что процессы не адаптированы к нуждам бизнеса. Требования бизнеса часто трансформируют в ИТ проекты, которые не могут работать вместе, возможность переиспользования артифактов, созданных для разных проектов зачастую очень низка. Создание приложений, которые были бы достаточно гибки для реагирования на неопределенность, требуют более систематического подхода к разработке самого приложения. Пока бизнес не сможет создать необходимый функционал для ИТ, который бы смог адекватно реагировать на неопределенность, традиционно сложно будет определить требования к размеру бюджета, необходимого для создания гиб-