3. Лагутин, М.Б. Наглядная математическая статистика. – Москва, 2007.
4. Baldock R., Graham J., Image Processing and Analysis A Practical Approach, Oxford, 2000.
5. Levkowitz H., Color Theory and Modelling for Computer Graphics, Vizualization, and Multimedia Applications, Norwell, 1997.
6. Корн, Г. Справочник по математике для научных работников и инженеров / Г. Корн, Т. Корн. – Москва, 1974.
7. Большаков, А.А. Методы обработки многомерных данных и временных рядов / А.А. Большаков, Р.Н. Каримов. – Смоленск, 2007.
8. Song Chun Zhu, Yuille A.L., FORMS: A Flexible Object Recognition and Modelling System, Harvard Robotics Lab. Technical Report no 94-101.
9. Gold C., Crust and Anti-Crust: A One-Step Boundary and Skeleton Extraction Algorithm, Quebec City.
10. Gonzales R.C., Woods R.E., Digital Image Processing, New Jersey, 2002.
11. Lam, L., Seong-Whan Lee, Ching Y. Suen, Thinning Methodologies-A Comprehensive Survey // IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol 14, No. 9, September 1992, page 879.
12. Павлидис, Т. Алгоритмы машинной графики и обработки изображений.

Материал поступил в редакцию 11.11.09

BUSHENKO D.A., SADYKHOV R.Kh. Modified algorithm of belt clustering for separation of crossing extended objects

There are various clustering algorithms which use different types of input data. The goal of the article is to develop a special clustering algorithm optimized for separation of crossing extended objects such as textile fibers. In this paper two types of algorithms are discussed and two most popular instances of these algorithms are observed: the C-means algorithm and the belt clustering algorithm. Since it is impossible to apply these algorithms for the task of separation of the crossed textile fibers, a special modification of the belt clustering algorithm is proposed. It is also presented a special space of descriptors whose effectiveness in separation of crossed extended objects is proved using the experimental results. Because of the fact that these descriptors contain nonuniform elements, it is also needed a special distance function. In this article it is proposed to use the Minkovsky distance. In conclusion, the comparison of the pure belt clustering algorithm and the modified one are discussed, and the advantages of the developed algorithm are shown in the task of separation of crossed extended objects.

УДК 004.8.032.26

Войцехович Л.Ю., Головко В.А., Курош Мадани

МУЛЬТИАГЕНТНАЯ СИСТЕМА ОБНАРУЖЕНИЯ АТАК С НЕЙРОСЕТЕВЫМ КЛАССИФИКАТОРОМ

Введение. Оперативный обмен информацией становится неотъемлемым атрибутом успешной деятельности в любой сфере. В последнее время прорыв в этой области обеспечили компьютерные технологии: компьютерные сети, электронная коммерция, корпоративные web-сайты и др. Однако наряду с необходимостью повышения надежности и скорости коммуникации остро встал вопрос обеспечения защиты информационных ресурсов.

Для защиты компьютерных систем применяются различные подходы. Все подходы можно разбить на две основные категории: организационные и технические. В свою очередь технические подходы подразделяются на сетевые и хостовые. Далее речь пойдет о сетевых средствах обеспечения безопасности, а именно, о системах обнаружения вторжений.

Задачей *Систем Обнаружения Вторжений* (*Intrusion Detection Systems – IDS*) является защита компьютерных сетей.

Наряду с правильной политикой безопасности, архитектурой межсетевых фильтров, антивирусным программным обеспечением и другими средствами IDS часто отводится роль основного элемента защиты. IDS используются в качестве средства раннего оповещения о сетевых проблемах. Это обусловлено размещением IDS в общей схеме обороны на сетевом уровне, на котором подозрительные действия могут быть обнаружены раньше, чем на более высоких уровнях. Кроме того, IDS способна предоставлять необходимые доказательства злоумышленных действий, а также выявлять скрытые тенденции, что становится возможным при анализе большого количества данных, обрабатываемых IDS.

К недостаткам существующих моделей IDS, в первую очередь, можно отнести уязвимость к новым атакам, низкую точность и скорость работы. Современные системы обнаружения вторжений плохо приспособлены к работе в реальном режиме времени, в то время как возможность обрабатывать большой объем данных в реальном времени – это определяющий фактор практического использования систем IDS. Указанные недостатки трудно устранить, используя только классические методы в области компьютерной безопасности. Поэтому в последнее время системы IDS активно изучаются. Разработчики систем обнаружения вторжений предлагают различные подходы: статистические методы [1, 2], нейронные сети [3, 4], деревья решений и SVM [5], генетические алгоритмы и искусственные иммунные системы [6, 7, 8, 9, 10].

В области обнаружения вторжений существует два основных метода: *обнаружение злоупотреблений* и *обнаружение аномалий*. Обнаружение злоупотреблений предполагает наличие сигнатур атак. Основным недостатком таких систем является их неспособность обнаруживать новые или неизвестные атаки, т.е. записи о которых в системе отсутствуют. Обнаружение аномалий [11] связано с построением профиля нормального поведения системы. При этом атакой считается любое отклонение от этого профиля. Главным преимуществом таких систем является принципиальная возможность определения ранее не встречавшихся атак.

Результаты исследований биологических механизмов *Иммунной системы человека* могут быть положены в основу построения систем обнаружения атак, поскольку базовые принципы работы в этих двух случаях схожи [12]. В иммунной системе человека имеются отдельные механизмы индивидуальной защиты и врожденного иммунитета, выполняющие функции аналогичные обнаружению злоупотреблений. Иммунная система человека состоит из различных иммунных клеток, химических сигналов, волокон и т.п. Их совместная работа позволяет обнаруживать определенные отклонения в организме человека, различать их и запускать необходимые механизмы иммунного ответа. А такие характеристики иммунной системы человека, как распределенность и самоорганизация (приспосабливаемость к изменчивым условиям), отвечают основным требованиям систем обнаружения аномалий. Таким образом, моделирование искусственной иммунной системы связано с разработкой алгоритмов динамического создания и обновления сигнатур, а так же алгоритмов обнаружения аномалий посредством сравнения с текущим состоя-

***Войцехович Леонид Юрьевич**, аспирант 3-го года обучения кафедры интеллектуальных информационных технологий Брестского государственного технического университета.*

***Головко Владимир Адамович**, д.т.н., профессор, зав. кафедрой интеллектуальных информационных технологий Брестского государственного технического университета.*

Беларусь, БрГТУ, 224017, г. Брест, ул. Московская, 267.

***Курош Мадани**, доктор наук, профессор университета Париж-XII.*

Франция, Париж, 12 Val de Marne (UPVM).

нием контролируемой системы.

В этой работе предлагается подход к построению *Мультиагентной системы с нейросетевым классификатором*, на базе совмещения механизмов *Искусственной иммунной системы* и *Искусственных нейронных сетей* с целью использования преимуществ обоих подходов. Предполагается, что такая система обнаружения атак будет способна выполнять обнаружение злоупотреблений и обнаружение аномалий в режиме реального времени.

Задача классификации – это основная задача в области обнаружения вторжений. Данная работа является продолжением предыдущих работ по созданию и исследованию систем обнаружения атак с нейросетевым классификатором [13, 14, 15].

Статья организована следующим образом: основные понятия из области иммунных систем рассматриваются в разделе 2; в разделе 3 приводится структура нейросетевого детектора, который предлагается использовать в этой работе; в разделе 4 дано концептуальное описание разрабатываемой мультиагентной системы (структура, функционирование). Проведенные эксперименты – в разделе 5. Основные результаты оговорены в заключительной части статьи.

Иммунная система. Перед тем как приступить непосредственно к рассмотрению искусственной иммунной системы для построения системы обнаружения атак, вкратце остановимся на работе иммунной системы человека. Это описание будет поверхностно, поскольку нас интересуют лишь те механизмы, которые можно использовать в области компьютерной безопасности.

Если так можно выразиться, то основным принципом работы иммунной системы человека является сравнение отдельных “образов” (шаблонов) с телами внутри организма человека. Таким образом, можно обнаружить инородные тела, которые называют антигенами.

В реальной жизни роль вышеупомянутых “шаблонов” выполняют лимфоциты. Они постоянно генерируются спинным мозгом и тимусом в соответствии с информацией, содержащейся в ДНК (эта информация накапливается, и такой процесс называется эволюцией генной библиотеки). Лимфоциты распространяются в организме через лимфатические узлы. Каждый тип лимфоцитов способен распознать некоторое ограниченное число антигенов. В процессе создания лимфоцитов имеется важный этап – *негативная селекция*. На этом этапе выполняется специальная процедура проверки на совместимость с родными клетками организма. Если лимфоцит несовместим, то он уничтожается. Иначе он будет бороться с клетками своего же организма. Таким образом, благодаря негативной селекции, “шаблоны” содержат информацию, которая отсутствует внутри организма. Если некоторое внешнее тело соответствует определенному “шаблону”, то оно воспринимается как инородное и должно быть немедленно уничтожено.

В случае если лимфоциты обнаруживают антиген, то на базе соответствующего шаблона создаются новые антитела, которые и уничтожают антиген. Существует также другой важный механизм – *клональная селекция*. Этот механизм подобен естественному отбору: выживают только те антитела, которые в наибольшей степени соответствуют обнаруженному антигену. Таким образом, данные о сформированных антителах попадают в так называемую иммунную память.

Одна из наиболее подходящих областей применения механизмов иммунных систем – это компьютерная безопасность, где аналогия между защитой человеческого тела и защитой нормально функционирующей компьютерной системы очевидна.

Эксперты, работающие в области искусственных иммунных систем, отмечают три основные свойства таких систем:

1 – во-первых, они распределенные;

2 – во-вторых, это самоорганизующиеся системы;

3 – в-третьих, такие системы не особенно требовательны к вычислительным ресурсам.

По мнению большинства экспертов, эффективная система обнаружения вторжений должна обладать всеми вышеперечисленными свойствами.

Нейросетевой детектор. В рассматриваемой мультиагентной системе обнаружения атак *нейросетевой детектор* (*классификатор*) выполняет функции лимфоцита в иммунной системе человека. Нейронные сети обладают хорошими обобщающими способностями, могут эффективно решать задачи аппроксимации, классификации и обработки зашумленных данных, что особенно важно в такой области, как обнаружение вторжений.

В данной работе в качестве основного агента системы обнаружения атак (см. рис. 1) предлагается использовать *нейронную сеть*, представляющую собой объединение *Рециркуляционной нейронной сети* (*Recirculation Neural Network - RNN*) и *Многослойного персептрона* (*Multilayer Perceptron – MLP*).

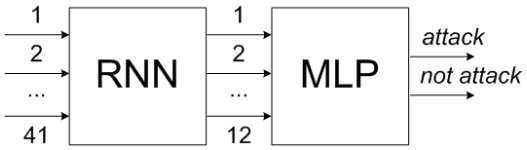

Рис. 1. Детектор для мультиагентной системы

На вход подается 41 параметр, определенный в базе KDD-99 [16]. Эта база содержит информацию о множестве соединений в компьютерной сети. RNN, применение которой с линейной функцией аналогично использованию метода главных компонент, выполняет сжатие 41 параметра входного вектора в 12-размерный выходной вектор. MLP обрабатывает полученные в результате сжатия значения и дает заключение относительно входного вектора, является ли он атакой определенного типа или же это нормальное соединение.

Такой детектор в проектируемой системе будет специализироваться на одном определенном типе атак. На выходе детектора возможны два состояния: “да” – если входной образ принадлежит заданному типу атаки, “нет” – входной образ не является атакой.

В мультиагентной системе можно использовать детекторы другого вида (рис. 2), детальное описание которых дано в наших предыдущих работах [13, 14, 15]. Но в дальнейшем мы будем ссылаться лишь на детектор, показанный на рис. 1.

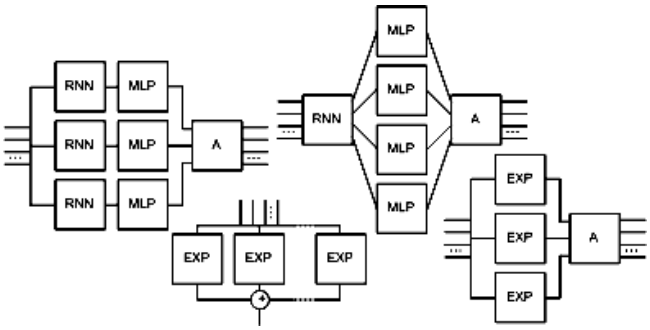

Рис. 2. Другие варианты построения нейросетевого детектора

После выполнения процедуры обучения нейронные сети могут использоваться в задаче обнаружения вторжений.

Мультиагентная нейронная сеть. В мультиагентной системе с нейросетевым классификатором (см. рис. 3) применяется множество детекторов, специализирующихся в различных областях знаний.

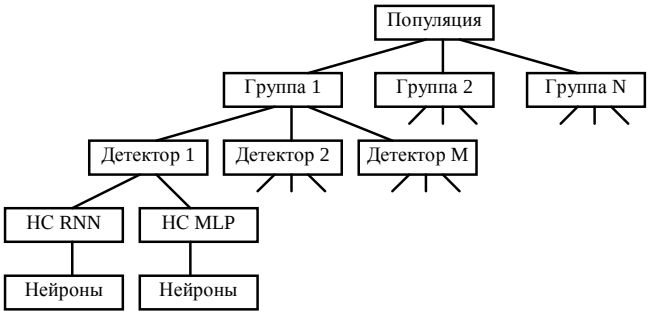

Рис. 3. Общая схема мультиагентной системы обнаружения атак

Реальные иммунные системы слишком сложны, чтобы можно было применить все имеющиеся в них механизмы защиты. Но в данном случае не требуются все возможности биологических иммунных систем. В ходе построения мультиагентной системы для обнаружения вторжений использованы лишь основные принципы и механизмы реальных иммунных систем, такие как: генерация и обучение детекторов с различной структурой и специализацией, отбор подходящих детекторов, возможность детекторов обнаруживать аномальную активность, клонирование и мутация детекторов, формирование иммунной памяти.

Рассмотрим обобщенную схему функционирования мультиагентной системы обнаружения вторжений (см. рис. 4).

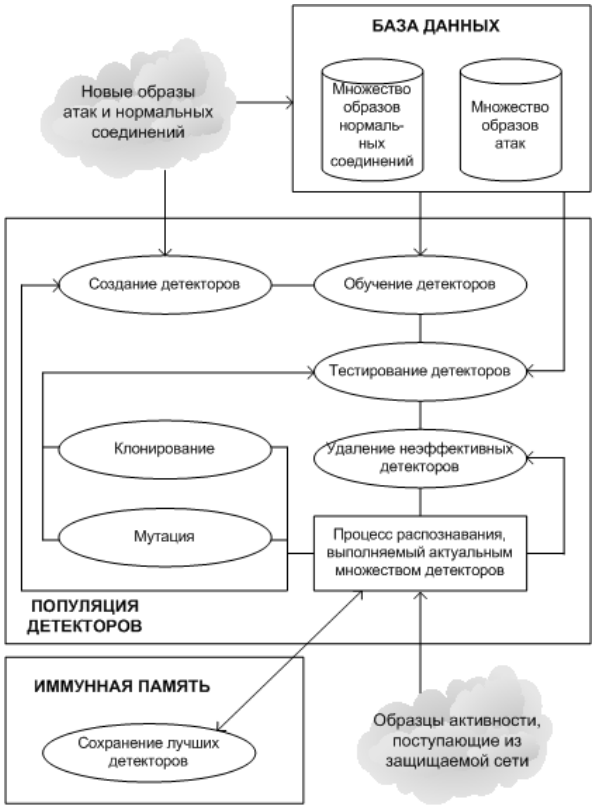

Рис. 4. Обобщенная схема функционирования разрабатываемой IDS

При инициализации системы все известные образы нормальной активности в сети, а также атак размещаются в двух базах данных – нормальных соединений и атак соответственно. Каждая запись в такой базе данных промаркирована либо как атака определенного типа, либо как не атака. Эти базы используются для формирования обучающих выборок нейросетевых детекторов и для тестирования системы обнаружения атак.

На следующем этапе инициализации системы обнаружения атак происходит создание популяции детекторов и выполняется процедура их обучения. Для формирования обучающей выборки отдельного детектора используются упомянутые выше базы данных сетевой активности.

Кроме того, необходимо предусмотреть специальную функцию контроля (проверки) текущего состояния системы обнаружения вторжений, чтобы "выбраковывать недообучившиеся" детекторы (такие детекторы сразу же должны удаляться из системы), и для расчета параметра эффективности отдельных детекторов.

Набор иммунных детекторов составляет популяцию, которая циркулирует в компьютерной системе и выполняет обнаружение и распознавание сетевых атак. Можно создавать сотни и тысячи детекторов, каждый из которых специализируется в своей области знаний и выполняет поиск характерных для него типов атак.

В процессе сканирования компьютерной сети детектор выполняет распознавание входного вектора, а совокупное заключение множества детекторов, составляющих популяцию, сообщается администратору сети, который и принимает решение, действительно ли наблюдаемая активность является атакой.

Динамические свойства предлагаемой системы обнаружения вторжений обусловлены постоянным обновлением детекторов в популяции. Это выполняется благодаря процедурам клонирования и мутации, пополнением популяции новыми детекторами и исключением из нее неэффективных или длительно используемых детекторов.

Образцы сетевой активности, используемые для настройки детекторов, оказывают сильное влияние на результаты процедуры обучения и на способность сформированных детекторов к обобщению. Таким образом, подбирая в обучающую выборку образы определенного типа, можно влиять на поведение создаваемых детекторов, на их способность к обнаружению образов того или иного типа.

В нашем случае процедура клонирования эквивалентна переобучению детектора, характеризующегося наименьшим значением параметра эффективности, на образах из обучающей выборки детектора с наивысшим значением данного параметра (предполагается, что оба детектора специализируются на одном и том же типе атак).

Под мутацией понимается процедура переобучения детектора, выбранного случайным образом из множества детекторов, составляющих популяцию.

Неэффективные детекторы и детекторы с истекшим временем жизни удаляются из системы или заменяются вновь сформированными детекторами.

В случае если детектор достигает наилучших показателей эффективности среди детекторов, специализирующихся в определенном типе атак, то информация о нем сохраняется в иммунной памяти системы (для детекторов, построенных на базе нейронной сети, сохраняются значения весовых коэффициентов). Эта информация может быть легко извлечена оттуда и использована для инициализации новых детекторов.

Как упоминалось выше, каждый детектор представлен искусственной нейронной сетью, состоящей из рецеркуляционной нейронной сети и многослойного персептрона, назначение которых оговаривалось выше.

Детекторы, которые работают с одним и тем же типом атак объединяются в группы от 3 до 10 детекторов. В общем случае предполагается, что детекторы в группе формируют различные заключения относительно входного образа, что является результатом случайных процессов в ходе обучения (для каждого детектора процесс обучения носит свой неповторимый характер). Теоретически количество детекторов в системе неограниченно и может легко изменяться в процессе выполнения программы, но в реальности могут возникать проблемы с производительностью компьютера (нехватка оперативной памяти, скорость и т.д.).

Процесс обработки подаваемого на вход системы вектора включает несколько этапов:

1. Входной образ попадает в мультиагентную систему.
2. Каждый детектор (или некоторое подмножество детекторов) дает свое заключение относительно поступивших данных.
3. Рассчитывается, так называемый, *фактор поддержки заключения* для каждой задействованной группы детекторов. Этот фактор отражает долю детекторов в группе, классифицирующих входной образ как атака определенного типа.
4. Выполняется сравнение факторов поддержки заключения, полученных для каждой группы детекторов. В качестве окончательного решения системы принимается заключение той группы, для которой фактор поддержки принимает наибольшее значение (процедура голосования).

Если поступает информация о новой атаке, отсутствующей в системе (например, от администратора или из другого источника), то записи о такой атаке добавляются в базу данных, и создается новая группа детекторов, которая будет работать в дальнейшем с данным типом атаки. Таким образом, происходит добавление в систему новых знаний.

К очевидным преимуществам рассмотренного подхода можно отнести:

1. Процедура обучения выполняется относительно просто;
2. Для обучения каждого отдельного детектора необходимо меньшее количество образов, чем в случае с моделями систем обнаружения атак, рассмотренных в предыдущих работах;

3. Это позволяет повысить качество обучения детекторов и значительно сократить время на подготовку очередного детектора.

Результаты тестирования. Для создания мультиагентной системы обнаружения атак была использована искусственная иммунная система.

При проектировании такой системы был решен ряд важных вопросов, а именно: получение коллективного решения на базе множества решений сгенерированных отдельными детекторами, метод селекции детекторов, выполнение клонирования и мутации, уничтожение непригодных или отработавших свой жизненный цикл детекторов... От того, как это делается, во многом зависит конечный результат работы такой системы.

В ходе проведения экспериментов рассчитывались следующие основные показатели эффективности IDS:

- количество обнаруженных атак (detected) – число записей, правильно классифицированных системой как атака;
- количество распознанных атак (recognized) – число записей, правильно классифицированных системой как атака, для которых верно определена принадлежность к определенному типу;
- количество ложных срабатываний системы – число записей, на которые система отреагировала как “атака”, но реакция оказалась ложной.

В ходе работы мультиагентной системы происходит множество случайных событий, определяющих ее поведение в текущий момент времени и в дальнейшем. Поэтому важно убедиться, что разработанная система обнаружения функционирует стабильно.

В связи с этим был проведен небольшой эксперимент. Под *стабильной работой* будем понимать то, что при каждом очередном цикле работы системы ее основные показатели эффективности (количество обнаруженных атак и количество ложных срабатываний) на одном и том же тестовом множестве не будут сильно разниться. В данном контексте под циклом подразумевается выполнение основных операций иммунной системы (клонирование, мутация, создание новых детекторов и замена существующих и т.п.).

Далее приведены результаты эксперимента. На рис. 5 в двумерном пространстве представлены результаты 50 циклов работы системы с некоторым тестовым множеством. Из рисунка следует, что такие показатели, как верное срабатывание и ложное срабатывание системы, не выходят за рамки определенных границ в течение длительного периода работы программы, т.е. система ведет себя относительно стабильно. Разброс точек на графике можно объяснить теми случайными процессами, которые имеют место в работе программы.

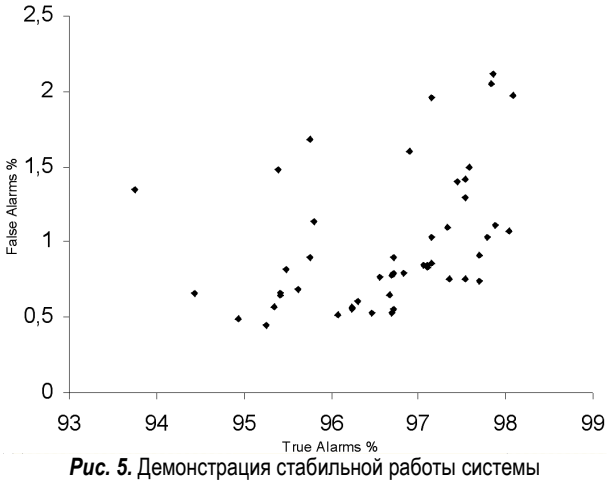

Рис. 5. Демонстрация стабильной работы системы

Рассмотрим функционирование мультиагентной системы на примере одной популяции детекторов. Допустим, популяцию составляют 110 детекторов. Причем на каждый определенный в KDD-99 тип записи в популяции приходится по 5-ть детекторов, которые образуют отдельную группу. Результаты эксперимента приведены в таблицах 1 и 2 и представлены в той же форме, что и в предыдущих работах [13, 14, 15]. Это позволяет сравнить результаты различных моделей системы обнаружения атак.

Таблица 1. Обучающая и тестовая выборка

	DoS	U2R	R2L	Probe	Normal	всего
Обучающая выборка	3571	37	278	800	1500	6186
Тестовая выборка	391458	52	1126	4107	97277	494020

Таблица 2. Обнаружение атак при помощи мультиагентной системы

класс	кол-во	обнаружено	распознано
DoS	391458	386673 (98.78%)	368753 (94.20%)
U2R	52	47 (90.39%)	45 (86.54%)
R2L	1126	1097 (97.42%)	930 (82.59%)
Probe	4107	4066 (99.00%)	4016 (97.78%)
Normal	97277	---	82903 (85.22%)

Записи об атаках класса DOS и Probe распознаны системой в более чем 90% случаев. Несколько хуже результат для соединений U2R и R2L. Также присутствуют так называемые ложные срабатывания системы.

Следующий эксперимент проведен с целью оценить реакцию системы на новые атаки (таблица 3). Под новыми атаками будем понимать те образы атак, которые изначально (при инициализации) не были включены в обучающую выборку. Для выполнения этого эксперимента был подготовлен отдельный набор записей для обучения и тестирования. Тестовая выборка включает все образы сетевых соединений из KDD тех служб, которые наиболее часто используются на практике, таких как HTTP, FTP, FTP_DATA, SMTP, POP3 и TELNET. Для обучения используется, как и в предыдущем эксперименте, выборка, включающая только часть записей из тестовой выборки, подготовленной для второго эксперимента. Причем информация об отдельных типах атак в ней вообще отсутствует. В этом эксперименте были полностью исключены из обучающей выборки записи о малочисленных атаках. Таким образом, в обучающей выборке представлено только 9 типов атак, а в тестовой - 18. Программой в процессе обучения в соответствии со структурой обучающей выборки были сформированы 9 отдельных групп детекторов по 5 в каждой группе. Численность популяции в данном случае составила 45 детекторов.

Таблица 3. Обнаружение атак при помощи мультиагентной системы (Шаг 1)

тип атаки	кол-во	обнаружено
Normal	75952	75269 (99.10%)
Back	2203	2157 (97.91%)
Neptune	901	899 (99.78%)
Buffer_overflow	30	28 (93.33%)
Loadmodule	9	8 (88.89%)
Guess_passwd	53	52 (98.11%)
Warezclient	1015	966 (95.17%)
Ipsweep	9	9 (100.00%)
Portsweep	15	14 (93.33%)
Satan	10	8 (80.00%)

Далее, предположим, что появилась информация о новом типе атак – “warezmaster”. Поступившую информацию необходимо внести в систему и сформировать новую группу детекторов, специализирующихся на этом типе атак. Для этого пополняем обучающую выборку записями о новой атаке. Автоматически при обновлении обучающей выборки система создает и подготавливает дополнительный набор детекторов, работающий с этим типом атаки. Так, в рассматриваемом примере после добавления “warezmaster” были сформированы и обучены 5 детекторов. Результаты работы системы с обновленной тестовой выборкой (учтены записи “warezmaster”) приведены в таблице 4.

Таблица 4. Обнаружение атак при помощи мультиагентной системы (Шаг 2)

тип атаки	кол-во	обнаружено
Normal	75952	75169 (98.97%)
Back	2203	2174 (98.68%)
Neptune	901	900 (99.89%)
Buffer_overflow	30	26 (86.67%)
Loadmodule	9	8 (88.89%)
Guess_passwd	53	53 (100.00%)
Warezclient	1015	947 (93.30%)
Warezmaster *	20	18 (90.00%)
Ipsweep	9	9 (100.00%)
Portsweep	15	14 (93.33%)
Satan	10	8 (80.00%)

* *– атаки, которые были добавлены в БД*

Изучим поведение системы в еще более сложной ситуации, когда на вход подаются образы атак, о которых системе "вообще ничего не известно", т.е. информация о таких атаках в базе данных системы отсутствует.

Таблица 5. Обнаружение атак при помощи мультиагентной системы (Шаг 3)

тип атаки	кол-во	обнаружено
Normal	75952	74340 (97.88%)
Back	2203	2169 (98.46%)
Land*	1	1 (100.00%)
Neptune	901	900 (99.89%)
Buffer_overflow	30	26 (86.67%)
Loadmodule	9	9 (100.00%)
Perl*	3	0 (0.00%)
Rootkit*	7	3 (42.86%)
ftp_write*	6	5 (83.33%)
guess_passwd	53	53 (100.00%)
Multihop*	7	5 (71.43%)
Phf*	4	0 (0.00%)
Spy*	2	0 (0.00%)
Warezclient	1015	981 (96.65%)
Warezmaster	20	19 (95.00%)
Ipsweep	9	9 (100.00%)
Nmap*	2	2 (100.00%)
Portsweep	15	15 (100.00%)
Satan	10	8 (80.00%)

* *– атаки, которые системе неизвестны*

Из таблицы 5 следует, что большое число записей о неизвестных системе обнаружения вторжений атаках были правильно классифицированы как "атака". Это свидетельствует о том, что такая мультиагентная система обладает способностью к обобщению и может использоваться для обнаружения ранее неизвестных типов активности в сети.

Заключение. В данной работе предложена концептуальная модель построения мультиагентной системы обнаружения на базе механизмов искусственных иммунных систем и искусственных нейронных сетей.

Такая система характеризуется: I) гибкостью, II) распределенностью, III) самоорганизацией, IV) возможностью дообучения в процессе работы.

Результаты обнадеживают, поскольку выполненная модель системы обнаружения атак продемонстрировала способность не только распознавать образы атак с достаточно высокой степенью точности (в отдельных случаях свыше 90%), но и обнаруживать ранее неизвестные ей атаки, что повышает ценность такой системы.

СПИСОК ЦИТИРОВАННЫХ ИСТОЧНИКОВ

1. D.J. Marchette. A statistical method for profiling network traffic // In Proceedings of the USENIX Workshop on Intrusion Detection and Network / 1999. – P.119–128.
2. D.J. Marchette. Computer Intrusion Detection and Network Monitoring: A Statistical View-Point // Springer – 2001.
3. J. Cannady. Artificial neural networks for misuse detection // In Proceedings of the 1998 National Information Systems Security Conference (NISSC'98) / October 5–8 – Arlington, VA, 1998. – P. 443–456.
4. Beghdad R. Critical study of neural networks in detecting intrusions // Comput. Secur. – 2008. - doi:10.1016/j.cose.2008.06.001.
5. Sandhya Peddabachigari, Ajith Abraham, Crina Grosan, Johnson Thomas. Modeling intrusion detection system using hybrid intelligent systems // Journal of Network and Computer Applications – 2007. – 30. – P.114–132.
6. Morton Swimmer. Using the danger model of immune systems for distributed defense in modern data networks // Computer Networks – 2007. – 51. – P.1315–1333.
7. Gerry Dozier, Douglas Brown, Haiyu Hou, John Hurley. Vulnerability analysis of immunity-based intrusion detection systems using genetic and evolutionary hackers // Applied Soft Computing – 2007. – 7. – P. 547–553.
8. Mohammad Saniee Abadeh, Jafar Habibi, Zeynab Barzegar, Muna Sergi. A parallel genetic local search algorithm for intrusion detection in computer networks // Engineering Applications of Artificial Intelligence – 2007. – 20. – P.1058–1069.
9. M. Saniee Abadeha, J. Habibia, C. Lucasb. Intrusion detection using a fuzzy genetics-based learning algorithm // Journal of Network and Computer Applications – 2007. – 30. – P.414–428.
10. S. Bezobrazov, V. Golovko. Neural Networks and Artificial Immune Systems – Malware Detection Tool // In Proceedings of the X International PhD Workshop OWD'2008 – Wisla, Poland, 2008. – P. 465–469.
11. Animesh Patcha, Jung-Min Park. An overview of anomaly detection techniques: Existing solutions and latest technological trends // Computer Networks – 2007. – 51. – P. 3448–3470.
12. U Aickelin, P Bentley, S Cayzer, J Kim, J McLeod. Danger Theory: The Link between AIS and IDS? // In Proceedings of ICARIS-2003, 2nd International Conference on Artificial Immune Systems / P.147-155.
13. V. Golovko and L. Vaitsekhovich. Neural Network Techniques for Intrusion Detection // In Proceedings of the International Conference on Neural Networks and Artificial Intelligence (ICNNAI-2006) / Brest State Technical University – Brest, 2006. – P. 65–69.
14. V. Golovko, P. Kachurka and L. Vaitsekhovich. Neural Network Ensembles for Intrusion Detection // In Proceedings of the 4th IEEE Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS-2007) / Research Institute of Intelligent Computer Systems, Ternopil National Economic University and University of Applied Sciences Fachhochschule Dortmund - Dortmund, Germany, 2007. – P. 578–583.
15. V. Golovko, L. Vaitsekhovich, P. Kochurko and U. Rubanau. Dimensionality Reduction and Attack Recognition using Neural Network Approaches // Proceedings of the Joint Conference on Neural Networks (IJCNN 2007) / Orlando, FL, USA – IEEE Computer Society, Orlando, 2007. – P. 2734–2739.
16. 1999 KDD Cup Competition. – Information on: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html.

Материал поступил в редакцию 22.11.09

VAITSEKHOVICH L.U., GOLOVKO V.A., KUROSH MADANI Multiagent system of detection of attacks with neural network by the qualifier

In this article the artificial immune system and neural network techniques for intrusion detection have been addressed. The AIS allows detecting unknown samples of computer attacks. The integration of AIS and neural networks as detectors permits to increase performance of the system security. The detector structure is based on the integration of the different neural networks namely RNN and MLP. The KDD-99 dataset was used for experiments performing. The experimental results show that such intrusion detection system has possibilities for detection and recognition computer attacks.