2. Лукацкий А. В. Обнаружение атак. – СПб.: БХВ-Петербург, 2003.
3. J. Cannady. Applying Neural Networks to Misuse Detection. In *Proceedings of the 21st National Information Systems Security Conference.*
4. J. M. Bonifacio et al. Neural Networks applied in intrusion detection systems, In *Proc. of the IEEE World congress on Comp. Intell.* (WCCI'98), 1998.
5. C. Jirapummin and N. Wattanapongsakorn. Visual Intrusion Detection using Self-Organizing Maps. In *Proc. of Electrical and Electronic Conference (EECON-24)*, Thailand, Vol. 2, pp. 1343-1349, 2001.
6. D. Joo, T. Hong and I. Han. The neural network models for IDS based on the asymmetric costs of false negative errors and false positive errors. *Expert Systems with Applications, 25 (2003)*, pp. 69-75
7. C. Zhang, J, Juang, M. Kamel. Intrusion detection using hierarchical neural networks. *Pattern Recognition Letters (2004).*
8. H. G. Kayacik. Hierarchical self organizing map based IDS on KDD benchmark. M. Sc. work, Dalhousie university, Halifax, Nova Scotia, 2003.
9. Головко В. А., Каменда Д. В., Кочурко П. А. Некоторые аспекты применения нейронных сетей для обнаружения сетевых атак *Вестник БГТУ. Физика, математика, информатика*. – 2004. - №5(29). – С. 35-39
10. П. Кочурко. Нейросетевой детектор аномалий. Известия Белорусской инженерной академии, № 1(19)/2'2005 – с. 78-81.
11. V. Golovko, P. Kochurko. Intrusion recognition using neural networks. *International Scientific Journal of Computing*, vol.4, issue 3, 2005, p.37-42
12. KDD Cup'99 Competition, 1999, http://kdd.ics.uci.edu/ databases/kddcup99/ kddcup99.html
13. Giacinto G., Roli F., Fumera G. Selection of image classifier. *Electron*, 26(5), 2000, pp. 420-422.
14. Xu L., Krzyzak A., Suen C. Y. Methods for combining multiple classifiers and their applications to handwriting recognition. *IEEE Trans. Syst. Man Cybernitics*, 22, 1992, pp. 418-435
15. Головко В. А. Нейронные сети: обучение, организация и применение. М.: ИПРЖР, 2001.
16. S. Hawkins, H. He, G. Williams, R. Baxter. Outlier Detection Using Replicator Neural Networks. In *Proc. of the 4th International Conference on Data Warehousing and Knowledge Discovery (DaWaK02) Lecture Notes in computer Science*, Vol. 2454, Springer, Pages 170-180, ISBN 3-540-44123-9, 2002
17. Giacinto G., Roli F., Didaci L. Fusion of multiple classifiers for intrusion detection in computer networks. *Pattern Recognition Letters*, 24, 2003, pp. 1795-1803
18. Lee W., Stolfo S. A Framework for Constructing Features and Models for Intrusion Detection Systems. *Information and System Security*, 3(4), 2000, pp. 227-261
19. Eskin E., Arnold A., Prerau M., Portnoy L., and Stolfo S. A Geometric Framework for Unsupervised Anomaly Detection: Detecting intrusiond in unlabeled data. In D. Barbara and S. Jajodia editors, *Applications of Data Mining in Computer Security.* Kluwer, 2002.
20. Pfahringer B. Winnings the KDD99 Classification Cup: Bagged Boosting. *SIGKDD Explorations*, 1(2), 2000, pp. 65-66.

УДК 004.8.032.26

Безобразов С.В.

ПРИМЕНЕНИЕ ИСКУССТВЕННЫХ ИММУННЫХ СИСТЕМ ДЛЯ ОБНАРУЖЕНИЯ ВИРУСОВ

ВВЕДЕНИЕ

Развитие новых информационных технологий предоставило не только уникальные возможности для более активного и эффективного развития экономики, политики, государства и общества, но и стимулировали возникновение и развитие компьютерной преступности. Ярким и наиболее опасным примером компьютерной преступности является написание и распространение компьютерных вирусов – автономно функционирующих программ, способных к самостоятельному внедрению в тела других программ, к последующему самовоспроизведению и самораспространению в информационно-вычислительных сетях и отдельных ЭВМ, и выполняющих нежелательные для пользователя ЭВМ действий [1].

Число компьютерных преступлений растет и, ущерб от них увеличивается (рис. 1).

Современные антивирусные программы не обеспечивают должный уровень защиты компьютерной системы от заражения вирусом. Традиционные антивирусные программы имеют ряд существенных недостатков. Рассмотрим наиболее серьезные из них:

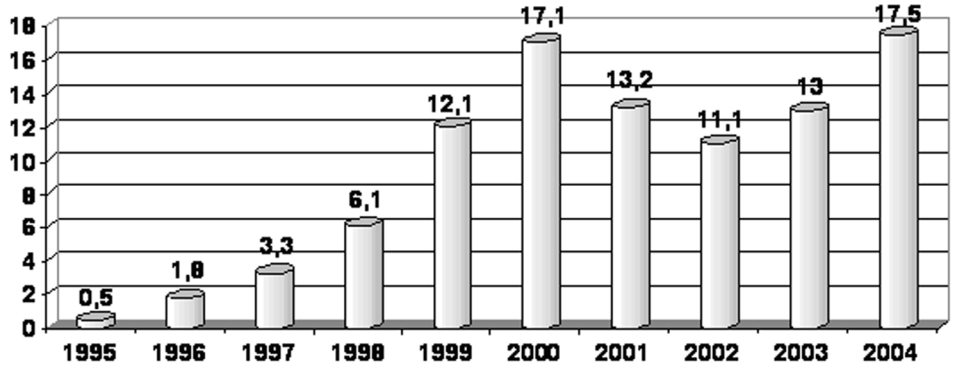

Рис. 1. Ущерб от компьютерных преступлений.

Безобразов С.В., *аспирант каф. интеллектуальных информационных технологий Брестского государственного технического университета.*
Беларусь, БрГТУ, 224017, Беларусь, г. Брест, ул. Московская, 267.

- нет никаких гарантий, что разработчики антивирусов не ошиблись и учли все возможные ситуации и модификации вирусов. Учитывая скорость пополнения антивирусных баз данных и малое время, отводимое специалистам на анализ новых вирусов, существует большая вероятность того, что множество деталей окажутся не замеченными, и антивирус будет работать не так как предполагается или вообще не будет работать;
- для успешного обнаружения вирусов необходимо иметь актуальные антивирусные базы, которые, как правило, располагаются на сайте разработчика антивирусной программы. На отслеживание обновления антивирусных баз и скачивания их с сайта уходит какое-то время. Последние вирусные эпидемии распространялись по всему миру всего за несколько часов, и антивирус с устаревшими базами может оказаться бессилен перед новой угрозой;
- существует вероятность того, что при загрузке антивирусной программы в оперативную память, уже имеющийся там вирус способен заразить сам антивирус. В результате, при сканировании системы на наличие вирусов, все проверяемы антивирусом файлы будут заражены этим вирусом;
- существующие эвристические алгоритмы, которые реализованы в современных антивирусных программах для обнаружения «неизвестных» вирусов, далеки от совершенства. На практике происходит так, что большинство пользователей чаще встречаются с ложными срабатываниями эвристических анализаторов, нежели с точными попаданиями и рано или поздно отключают эвристический анализатор [2].

Все это послужило толчком для поиска нестандартных, нетрадиционных путей для обеспечения компьютерной безопасности. В природе существует идеальный механизм защиты биологического организма от болезней, которые распространяются болезнетворными микробами. Этим механизмом является биологическая иммунная система. Иммунная система человека с успехом обнаруживает и борется с огромным количеством как известных, так и неизвестных вирусов каждый день. Если основные механизмы иммунной системы человека неким образом перенести на компьютерную платформу, то мы получим такую систему защиты, которая будет лишена главного недостатка существующих систем безопасности – неспособность распознавать «неизвестные» вирусы.

Применение метода искусственных иммунных систем для обнаружения аномалий (вирусов), основанный на принципах биологической иммунной системы, наряду с традиционными способами защиты информации существенно повысит уровень защищенности компьютерных систем.

БИОЛОГИЧЕСКАЯ ИММУННАЯ СИСТЕМА

Биологическая иммунная система (иммунная система человека) успешно защищает организм от болезнетворных бактерий посредством специфического реагирования на присутствие этих бактерий. Эта способность чрезвычайно важна для организма. Замечательно то, что иммунная система способна обнаруживать не только «известные» ей вирусы (врожденный иммунитет), но и не известные, ранее не встречающиеся в организме, вирусы (приобретенный иммунитет). Иммунитет основан на синтезе специальных белков, так называемых антител, способных вступать в соединение с чужеродными веществами – антигенами. Упрощенный механизм биологической иммунной системы изображен на рисунке 2.

Основными элементами иммунной системы являются лимфоциты – белые клетки [3]. Лимфоциты образуются из стволовых клеток в костном мозге. После синтеза лимфоциты направляются к органам, в которых происходит их созревание: тимусу (вилочковой железе) и лимфатическим узлам. Лимфоциты в зависимости от места их созревания делятся на В-лимфоциты и Т-лимфоциты. Зрелые лимфоциты имеют на своей поверхности детекторы, которые способны обнаруживать специфический антиген (вредные бактерии, вирусы).

Контакт В-клеточных рецепторов со специфическим антигеном и связывание определенного его количества стимулируют рост этих клеток и последующее многократное деление. В результате образуются многочисленные клетки двух разновидностей: плазматические и «клетки памяти». Плазматические клетки синтезируют антитела, тем самым, увеличивая количество клеток, способных обнаруживать вирус. Клетки памяти являются копиями В-клеток, однако имеют гораздо больший период жизни, что обеспечивает защиту организма от повторного заражения вирусом.

При связывании определенного количества вируса, Т-клетки секретируют особую группу веществ, называемую

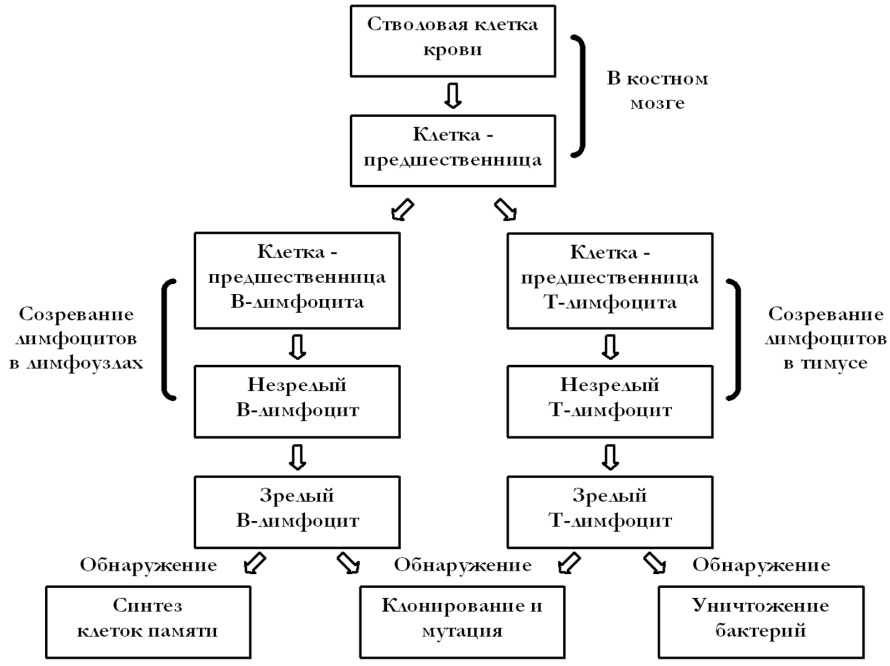

Рис. 2. Биологическая иммунная система.

лимфокинами. Некоторые лимфокины способны сами разрушать антиген и зараженные клетки. Другие лимфокины способствуют делению Т-клеток, в результате чего появляется большое количество антител, способные реагировать на обнаруженный антиген.

Биологическая иммунная система обладает рядом свойств, которые необходимы для успешной защиты информации в компьютерных системах – распределенность, динамичность, адаптивность.

ИСКУССТВЕННАЯ ИММУННАЯ СИСТЕМА

В отличие от биологического тела, компьютерная среда не постоянна. Она находится в постоянном изменении: устанавливается новое программное обеспечение, удаляется старое, появляются новые файлы. Для успешного обнаружения вирусов необходимо находить отличие между компьютерными вирусами и файлами системы. Анализируя структуры различных вирусов, мы пришли к следующему выводу: так как все вредоносные программы направлены на нарушение нормального функционирования системы, они по своей структуре (определенному набору команд) разительно отличаются от файлов системы – «чистых» файлов. Основную роль в искусственной иммунной системе по обнаружению вирусов играют антитела (детекторы), которые способны распознавать вредоносные программы.

Искусственная иммунная система строится по основным принципам биологической иммунной системы и состоит из следующих процессов: генерация антител, селекция антител, циркуляция антител в системе, клонирование и мутация, создание иммунной (генетической) памяти. Рассмотрим подробнее каждый механизм иммунной системы. Механизм искусственной иммунной системы представлен на рисунке 3.

Генерация антител. Механизм генерации антител представляет собой случайный процесс. Суть его заключается в том, чтобы сгенерировать такую последовательность бит, которая по своей структуре была бы максимально схожа со структурой возможного вируса. Антитела генерируются в двоичном виде, так как информация, а, следовательно, и вирусы в компьютерной системе, хранится в двоичном виде. При генерации детекторы наделяются такими свойствами как жизненный цикл и размерность. Жизненным цикл – это некий промежуток времени, в течение которого антитело находится (живет) в компьютерной системе. Он необходим для предотвращения переполнения системы антителами (что негативно отразится на общей производительности системы), а также для появления в системе большого количества разнообразных по своей структуре антител. Если, по истечении жизненного цикла, детектор не обнаружил вирус, он уничтожается, а на его место приходит другой. Если во время жизненного цикла детектор обнаружил аномалию (вирус или зараженный файл), то его жизненный цикл продлевается.

Немаловажным критерием детектора является размерность – количество бит в битовой строке детектора. Если взять недостаточную размерность, то неизбежно возрастут ложные срабатывания - детектор вместо вирусов будет реагировать на чистые файлы. Если размерность окажется слишком большой, то время, необходимое для детекции возрастет за счет увеличения количества проверок, что приведет к нежелательной загрузке компьютерной системы. В традиционных антивирусных пакетах размер сигнатуры (уникальной строки бит, которая однозначно характеризует ту или иную вредоносную программу) составляет от 64 до 512 бит [2].

Следует отметить, что детектор является полностью независимым объектом, т.е. в искусственной иммунной системе не существует некоего единого центра управления, который бы указывал детектору, какой файл ему необходимо проверить. Каждый детектор выбирает сам (например, случайным образом) файл для проверки. Отсутствие единого центра управления обеспечивает защиту иммунной системы от заражения ее каким-либо вирусом.

Селекция антител. Детекторы генерируются случайным образом, поэтому существует вероятность того, что некоторые из них, вместо вирусов, будут реагировать на чистые файлы. Механизм селекции предотвращает попадание нежелательных антител в систему. Наиболее распространенным алгоритмом селекции является алгоритм негативной селекции, предложенный С.Форест [4]. Сгенерированные антитела проверяются на способность детекции чистых файлов. Если детектор реагирует на тестовый чистый файл, то он считается негативным детектором и удаляется. Выживают только те детекторы, которые не реагируют на тестовые чистые файлы. Эти детекторы циркулируют по системе и выполняют свою

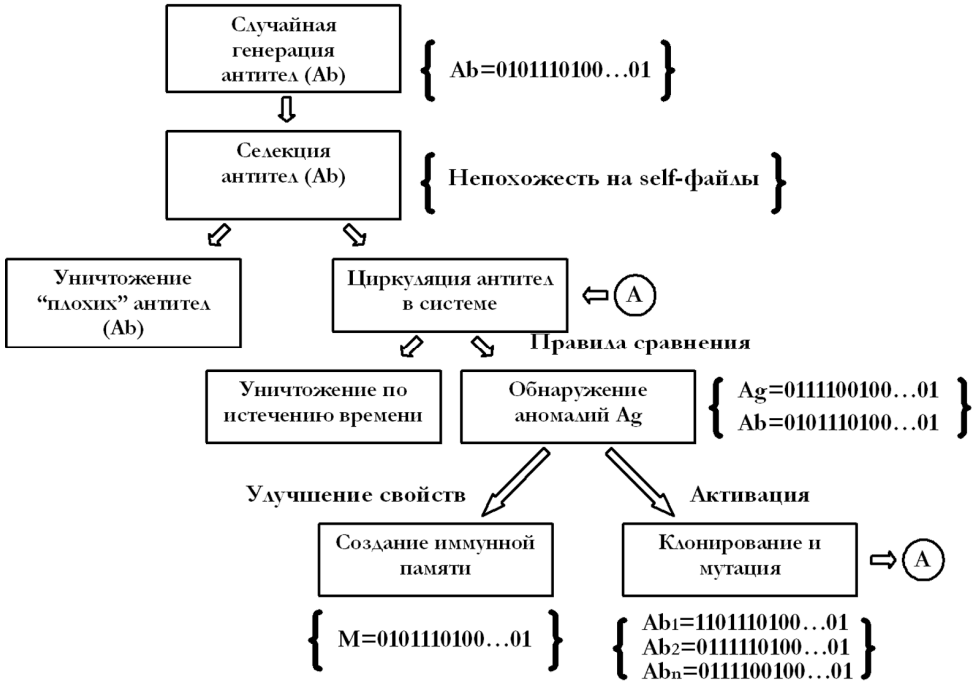

Рис. 3. Искусственная иммунная система. *Ag* – аномалия, *Ab* – антитело, *M* – клетка памяти.

иммунологическую функцию. Алгоритм негативной селекции можно представить следующим образом:

- определяем набор *S* чистых файлов в неком пространстве;
- случайным образом генерируем множество детекторов *R*;
- сравниваем каждый детектор из множества *R* с чистыми файлами из *S*;
- если детектор и чистый файл достаточно похожи, то удаляем детектор из *R*, иначе «выпускаем» детектор в систему.

Циркуляция антител в системе. На протяжении жизненного цикла антитела циркулируют внутри компьютерной системы, выполняя свою защитную функцию.

Для проверки файлов можно использовать несколько алгоритмов. Наиболее простым из них является правило r-смежных бит, который был предложен С.Форест [4] (рис. 4). Суть его заключается в следующем: если две битовых строки *R* и *S* имеют *r* идентичных смежных бит, то происходит обнаружение, иначе обнаружения нет. Параметр *r* называется порогом.

Если в течение жизненного цикла происходит обнаружение вируса, детектор подает соответствующий сигнал. Большинство компьютерных вирусов, проникая в систему, заражает большое количество файлов операционной системы. Для того чтобы как можно скорее очистить компьютерную систему от обнаруженного вируса, необходимо большое количество копий детектора, который произвел обнаружение.

Процесс создания большого количество копий детектора, который обнаружил вирус в системе, называется клонированием. Копии называются клонами, а детектор, который обнаружил вирус, называется родителем. Для того, чтобы клоны были максимально схожи с найденным вирусом, клоны подвергаются незначительной мутации. Это делается путем внесения незначительных изменений в структуру клона. Если свойства клона улучшаются, то он сам в свою очередь может стать родителем. Если же свойства клона в результате мутации ухудшаются, то он удаляется из системы.

При обнаружении вируса, в системе появляется большое количество антител, которые схожи по структуре и все они реагируют на найденный вирус. Искусственная иммунная система адаптируется под вирус, стараясь как можно скорее «вылечить» систему. После уничтожения вируса, клоны постепенно «умирают», так как имеют ограниченный жизненный цикл, и искусственная иммунная система переходит в свое нормальное состояние.

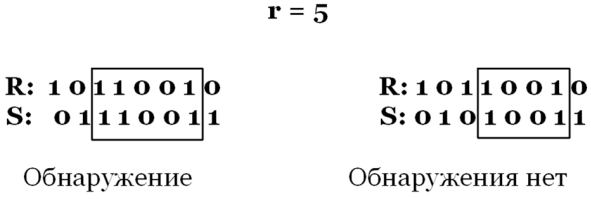

Рис. 4. Правило r-смежных бит. *R* – детектор, *S* – проверяемая строка, *r* – порог.

Иммунная память. Иммунная (генетическая) память предназначена для длительного хранения информации о предыдущих заражениях системы и является механизмом быстрого реагирования на повторные заражения системы. Носителями этой информации являются совокупность клеток памяти. Клетки памяти являются копиями детекторов, которые обнаруживали вирусы. Однако в сравнении с обычными детекторами, клетки памяти обладают улучшенными характеристиками. Они имеют гораздо больший жизненный цикл, а также меньший порог срабатывания. С помощью данного механизма искусственная иммунная система быстро и четко справляется с повторным заражением компьютерной системы.

РЕЗУЛЬТАТЫ

Была реализована простейшая иммунная система для обнаружения вирусов. Внимание акцентировалось на изучение способность искусственной иммунной системы, отличать чистые файлы от вредоносных программ. Искусственная иммунная система случайным образом генерировала 500 антител. После чего все они сравнивались с файлом. Наиболее похожий детектор сравнивался с «чистыми» файлами. Анализ полученных результатов выявил неспособность антител, сгенерированных случайным образом, распознавать вирусы. Для устранения этого недостатка, в процессе обучения был реализован простейший генетический алгоритм. Суть его заключалась в следующем: из 500 сгенерированных случайным образом детекторов выбираются детекторы, обладающие лучшими свойствами, которые в дальнейшем участвуют в формировании следующего поколения. Остальные уничтожаются. Полученные результаты приведены в таблице 1.

Результаты показали, что использование генетического алгоритма в механизме обучении детектора, наделяет детектор способностью распознавать вирус. Рис. 5 показывает улучшение свойств детектора на этапах генетического алгоритма.

ВЫВОДЫ

Искусственная иммунная система позволяет использовать совершенно новые подходы в обнаружении вредоносных программ. Она обладает такими необходимыми для системы защиты свойствами, как: распределенность, многообразие, обнаружение неизвестных вирусов, динамичность, адаптивность, отсутствие единого центра управления. Мы полагаем, что система безопасности, построенная на основе искусственной иммунной системе, поможет ликвидировать проблемы, существующие на современном этапе развития традиционных антивирусных продуктов, и повысит уровень защиты компьютерных систем.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Антивирусные «движки» – http://www.avinfo.ru, 2005.
2. Почему не срабатывают антивирусы – http://www.i2r.ru, 2003.
3. Иммунитет – http://krugosvet.ru, 2004.
4. Gonzlez, Fabio. A study of Artificial Immune Systems Applied to Anomaly Detection // PhD. Dissertation, The University Of Memphis, May 2003.

Таблица 1.

	файл-вирус	dll - файлы	txt - файлы	zip - файлы	exe - файлы	log - файлы	doc - файлы	bmp - файлы
Случайная генерация	10	10	10	10	10	10	9	8
Генетический алгоритм	33	13	15	10	13	15	8	11

Примечание: значения совпадений в таблице 1 даны в процентном соотношении от длины детектора (длина детектора = 256).

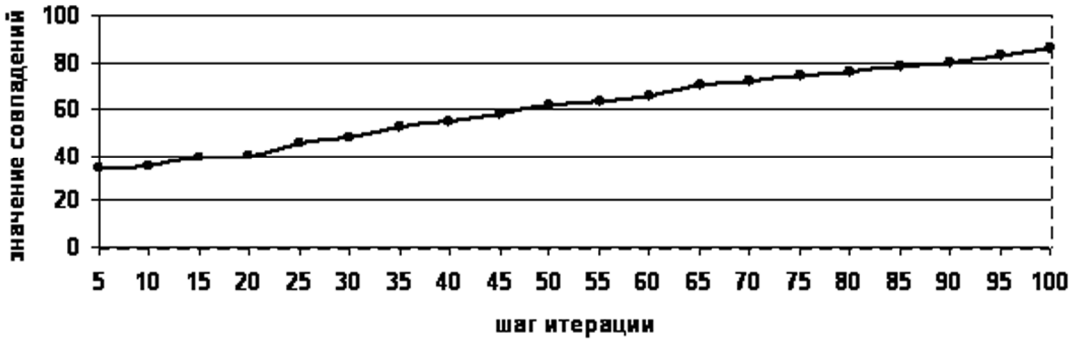

Рис. 5. Генетический алгоритм.

УДК 621.3

Майкив И.М, Кочан Р.В., Кочан В.В., Саченко А.О., Турченко И.В.

СЕТЕВОЙ ПРИКЛАДНОЙ ПРОЦЕССОР, РЕАЛИЗОВАННЫЙ НА ПРОГРАММИРУЕМОЙ ЛОГИЧЕСКОЙ МАТРИЦЕ

ВВЕДЕНИЕ

Усложнение алгоритмов обработки данных в системах управления технологическими процессами требует использования многопроцессорных иерархических систем. Поэтому, современные измерительно-управляющие системы строятся в виде локальных сетей с распределенными вычислительными ресурсами. Базовым элементом таких сетей является сетевой процессор (СП), выполняющий ряд заданных функций, связанных с обработкой сенсорных данных и взаимодействием с другими узлами сети.

Области использования таких систем и решаемые задачи весьма разнообразны. Поэтому СП должны быть многофункциональными элементами, способными обеспечить обработку данных в реальном времени и прозрачный обмен результатами в сети. Поскольку оборудование автоматизации технологических процессов выпускает множество фирм, на первый план выступают вопросы унификации интерфейсов и протоколов взаимодействия на всех уровнях сети. Их решение обеспечит открытость, гибкость, масштабируемость сетей, возможность их адаптации к различным реальным задачам, долгий жизненный цикл оборудования.

Стандарты, унифицирующие требования к интерфейсам на аппаратном уровне, известны уже давно и постоянно усовершенствуются [1]. В тоже время стандарты, устанавливающие требования к программному обеспечению и протоколам организации взаимодействия в таких сетях, появились значительно позже, и их внедрение вызывает определенные трудности. В результате, СП различных производителей зачастую не совместимы между собой на программном уровне.

Для решения этой проблемы была разработана серия стандартов IEEE-1451 [2-4], регламентирующая требования к обеспечению аппаратной и программной совместимости элементов распределенных измерительно-управляющих сетей. Структура такой сети, удовлетворяющая требованиям IEEE-1451, включает (рис. 1):

1. Интерфейсные модули преобразователей (ИМП) – узлы нижнего уровня сети, к которым непосредственно подключаются сенсоры и исполнительные механизмы;
2. Сетевые прикладные процессоры (СПП) – промежуточный уровень сети, управляют работой ИМП, и обрабатывают текущие данные, поступившие из ИМП;
3. Центральный сервер – верхний уровень сети, обеспечивает ее функционирование. Сюда же включены и другие потребители информации.

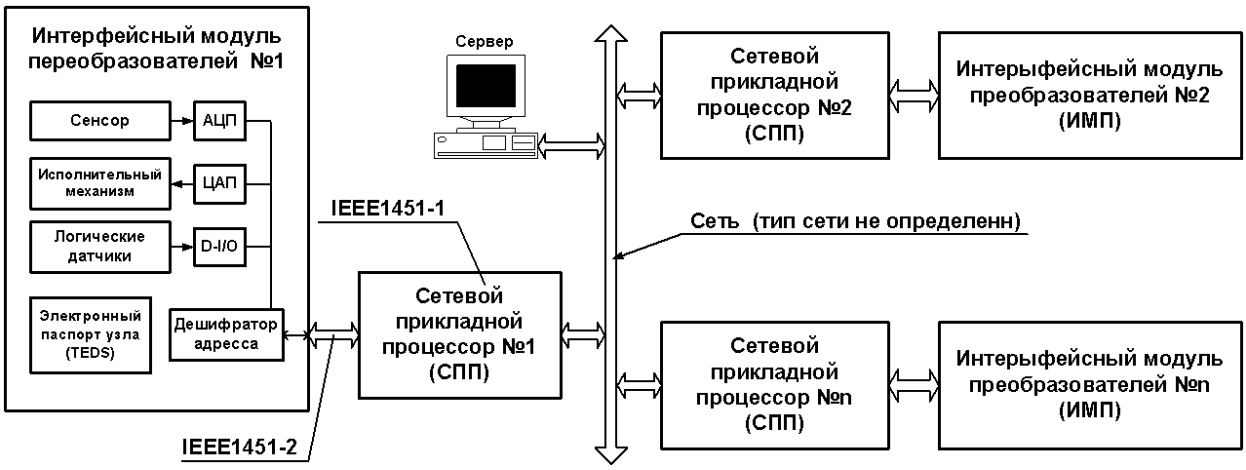

Рис. 1. Структура сети в соответствии с требованиями IEEE-1451.

Майкив И.М, Кочан Р.В., Кочан В.В., Саченко А.О., Турченко И.В., *Научно-исследовательский институт Интеллектуальных компьютерных систем.*
Украина, 46000, г. Тернополь, ул. Львовская, 11. mim@tanet.edu.te.ua