$$\text{найти } \max \overline{W}\left(x_{ij};\ i=\overline{1,n};\ j=\overline{1,m}\right) \qquad (17)$$

при ограничении $C\left(x_{ij}\right) \le C_{доп};\ i=\overline{1,n};\ j=\overline{1,m}$.

В работе [4] предлагается подход к формальному определению угроз информации.

В соответствии с формулировкой задачи (17) основными этапами ее решения являются:

– сбор и обработка экспертной информации о характеристиках угроз: частоте появления *i*-й угрозы $\overline{\lambda_i}$ и ущербе $\Delta q_i \ \left(i=\overline{1,n}\right)$;
– сбор и обработка экспертной информации для определения важности выполнения *j*-го требования для устранения *i*-угрозы α_{ij} и функции принадлежности $\mu\left(x_{ij}\right),\ \left(i=\overline{1,n};\ j=\overline{1,m}\right)$;
– оценка стоимости СЗИ для конкретного варианта ее реализации, зависящая от степени выполнения требований $C\left(x_{ij};\ i=\overline{1,n};\ j=\overline{1,m}\right)$;
– разработка математической модели и алгоритма выбора рационального варианта построения СЗИ (рационального задания требований) в соответствии с постановкой (17) как задачи нечеткого математического программирования.

III Выводы

В статье рассмотрен метод постановки формальной задачи синтеза системы защиты информации и основные этапы ее решения, а также показатели качества функционирования СЗИ – вероятность появления угроз, вероятность устранения угроз, предотвращенный ущерб за счет ликвидации угроз.

Литература: ***1.*** *Домарев В. В. Безопасность информационных технологий. Методология создания систем защиты.– К.: ООО "ТИД "ДС", 2001.* ***2.*** *НД ТЗИ 1.1-002-99. Общие положения по защите информации в компьютерных системах от несанкционированного доступа. // Департамент специальных телекоммуникационных систем и защиты информации Службы безопасности Украины. – Киев, 1999.* ***3.*** *НД ТЗИ 1.1-003-99. Терминология в области защиты информации в компьютерных системах от несанкционированного доступа. //Департамент специальных телекоммуникационных систем и защиты информации Службы безопасности Украины. – Киев, 1999.* ***4.*** *Антонюк А., Жора В. Моделювання доступу та каналів витоку в інформаційних системах //Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2001. Вип. 3. С. 156–160.*

УДК 681.3.067

ИСПОЛЬЗОВАНИЕ МУЛЬТИАГЕНТНЫХ СИСТЕМ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИОННЫХ РЕСУРСОВ КОМПЬЮТЕРНЫХ СЕТЕЙ

Александр Хошаба
Винницкий государственный технический университет

Аннотация: **Определены задачи и основные функции, стоящие перед средствами управления и контроля компьютерными сетями при защите информационных ресурсов. Детально описана структура мультиагентной системы, выполняющей защиту данных в компьютерных сетях.**
Summary: **In article problems and the basic functions which face to control facilities and the control in computer networks at protection of information resources are determined. The structure of multiagent system which carries out protection of the data in computer networks in details is described.**
Ключевые слова: **Защита информационных ресурсов компьютерных сетей, интеллектуальные технологии, мультиагентные системы.**

I Введение

В течение ряда лет в области искусственного интеллекта (ИИ) происходят революционные преобразования. Источниками этих преобразований служат распределенный искусственный интеллект (РИИ)

и активный объектно-ориентированный подход (АООП). Центральной идеей РИИ является кооперативное взаимодействие распределенных интеллектуальных систем. Подобластью РИИ являются мультиагентные системы (МАС).

Для построения МАС принято рассматривать агентов как автономные компоненты, действующие по определенному сценарию. Классифицируются агенты по четырем основным типам: простые (simple), умные (smart), интеллектуальные (intelligent) и действительно интеллектуальные (truly intelligent) [1].

Значительный интерес для построения МАС представляют интеллектуальные и действительно интеллектуальные агенты, которые отличаются тем, что поддерживают помимо функций автономного выполнения операции взаимодействия с другими агентами и мониторинг окружающей обстановки работы программных средств. Также считается [2], что к дополнительным возможностям в работе интеллектуальных и действительно интеллектуальных агентов можно отнести их способность использовать абстракции, адаптивность поведения, обучение на прецедентах и толерантность к ошибкам.

Интеллектуальные агенты (ИА) обладают такими основными свойствами [3]:

- автономность, то есть способность функционировать без постороннего вмешательства и осуществлять контроль внутреннего состояния и своих действий;
- социальное поведение – возможность взаимодействия с другими агентами;
- реактивность – реагирование на изменение среды;
- активность – способность генерировать цели и достигать их;
- базовые знания – начальные знания агента о среде;
- убеждения – значения переменных агента;
- цели – совокупность состояний, на достижение которых направлена деятельность агента;
- обязательства – задачи, которые агент может принять к исполнению;
- желания – состояния, контролируемые агентом;
- намерения – задачи, которые агент обязан выполнять в ходе своей деятельности.

Использование МАС или ИА наиболее эффективно при построении сложных систем. В данном случае, под сложной системой понимаются информационные структуры, в которых применение технологии “клиент-сервер” затруднительно или практически невозможно. В связи с тем, что защиту информационных ресурсов можно отнести к сложным системам, рассматривается подход [4–6] к созданию МАС для задач управления потоком данных и защиты данных в компьютерных сетях.

II Задачи, стоящие перед средствами управления потоком данных и защитой данных в компьютерных сетях

К наиболее важным задачам средств управления потоком данных и защитой данных в компьютерных сетях можно отнести такие:

общее управление сетью, в основу которого входит обеспечение функционирования программно-технических систем, собирающих данные о состоянии хостов (узлов) и коммуникационных устройств компьютерной сети; важными здесь являются автоматические или автоматизированные операции по включению и отключению портов устройств, изменению основных параметров и адресных таблиц мостов, коммутаторов, маршрутизаторов и т. п.;

сетевая обработка данных, которая состоит в управлении потоком данных и контроле потоков данных, непосредственно обрабатываемых на интерфейсах устройств;

управление конфигурацией сети, в функции которого входит конфигурирование компонентов компьютерной сети, включая взаимное расположение отдельных устройств, обработка сетевых адресов и идентификаторов, управление параметрами сетевых операционных систем, поддержка и сопровождение общей схемы сети;

обработка ошибок, которая характеризуется своевременным выявлением, определением и устранением последствий сбоев и отказов в работе компьютерной сети;

анализ производительности, в цели которого входят обработка статистической информации о важных параметрах функционирования сети: оценка времени ответа системы, величина и загруженность трафика;

управление безопасностью, включающая в себя общие аспекты контроля доступа и сохранения целостности данных; в цели данной задачи входит процедура аутентификации, проверка привилегий, поддержка ключей шифрования, управление полномочиями; сюда же относят механизмы управления паролями, внешним доступом, соединение с локальными или корпоративными компьютерными сетями;

учет работы сети, которая включает в себя регистрацию и управление используемыми ресурсами и устройствами; здесь важно учитывать параметры времени работы устройств и платы за использованные информационные ресурсы.

В работах [7–14] предлагаются подходы к решению перечисленных выше задач. Однако при этом отсутствует их комплексное решение, что наиболее важно при защите информационных ресурсов в компьютерных сетях. Комплексное решение указанных задач предлагается осуществить на основе интеллектуальных технологий, в частности МАС.

III Реализация системы управления потоком данных в компьютерных сетях на основе методов искусственного интеллекта

Система управления потоками данных (СУПД) в корпоративной или глобальной компьютерной сети представляет собой программно-аппаратный комплекс, построенный на базе технологий “клиент-сервер” и методов искусственного интеллекта – мультиагентных систем (рис. 1), в задачи которого входят:

- управление потоками данных в компьютерных сетях;
- мониторинг потоков данных в компьютерных сетях;
- защита информационных ресурсов локальных корпоративных и глобальных компьютерных сетей.

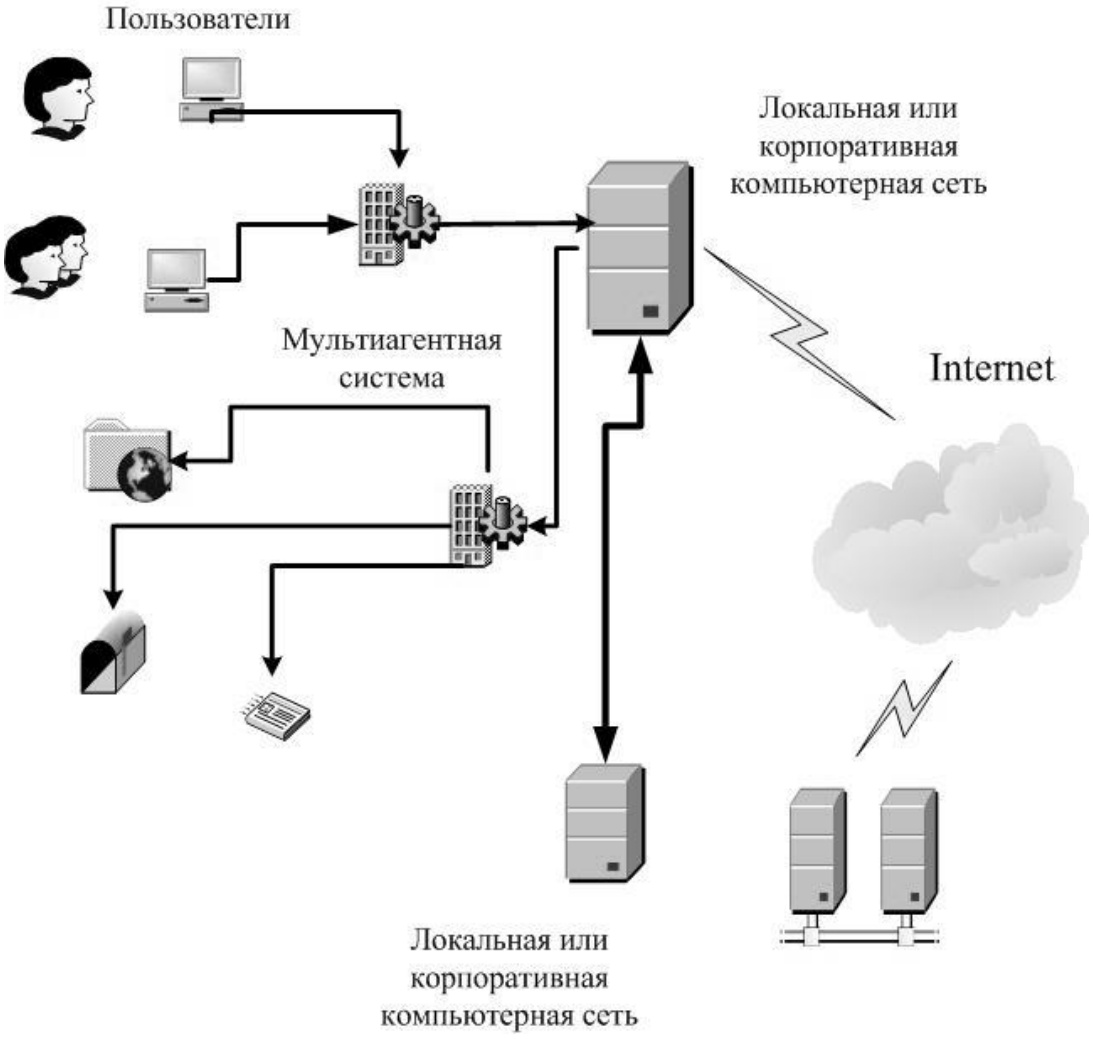

Рисунок 1 – Структура системы управления потоками данных в корпоративной или глобальной компьютерной сети

Управление потоками данных и мониторинг потоков данных в компьютерных сетях обеспечивался программными средствами, состоящими из операционной системы, прикладных программ и современных информационных технологий. При построении СУПД использовались распространенные операционные

системы Windows, Unix, прикладные программы, работающие на соответствующих платформах, интеллектуальные информационные технологии.

Аппаратные средства представляли собой персональные IBM PC-совместимые компьютеры. Практика последних десятилетий показала достаточную эффективность решений многих задач с использованием данного класса машин.

Для построения концептуальной модели системы управления потоками данных в корпоративной или глобальной компьютерной сети Internet необходимо было абстрактное выделение трех функциональных уровней.

Первый уровень составляли клиентские информационные ресурсы и средства управления локальными, корпоративными или глобальными компьютерными сетями. К ним относились:

- информационные ресурсы серверов (в качестве предоставления данных WWW, FTP, e-mail и т. д.);
- информационные ресурсы рабочих мест (в качестве потребителя информации);
- механизмы, обеспечивающие безопасность информационных ресурсов и управление (фильтрация) потоками данных. К примеру, программные средства ipfw и ipfilter – для операционной системы FreeBSD, ipchains – для операционной системы Linux.

При функционировании СУПД осуществляется фильтрация информационных входящих и исходящих потоков по заданным протоколам, портам, IP-адресам отправителя и получателя. При этом, все системы фильтрации и защиты данных были расположены на серверах локальных, корпоративных или глобальных узлов и являлись полностью автономными по отношению к другим системам последующих слоев.

Второй уровень представлял собой МАС, выполняющую функцию управления. Основными задачами данного уровня являлись:

- динамическое распределение функции управления, мониторинга и контроля потоков данных различных серверов;
- осуществление всех фаз взаимодействия с интеллектуальными агентами (формализация запроса управления и получения результата на выполнение конкретных операций).

МАС осуществляла передаточные и проверочные функции относительно информационных потоков от пользователя или конечной (клиентской) системы (потребителя информации) до управляемых ресурсов. Одной из составных частей МАС являлись интеллектуальные агенты (ИА). Предпочтительное место расположения МАС и ИА – сервера операционной системы Unix.

К третьему уровню относились сервера или системы управления базами данных/знаний, ориентированные на запросы пользователей, интеграцию и хранение результатов работы МАС или ИА. Основной задачей данного уровня являлись:

- предоставление пользователям возможности на формирование запросов;
- интерпретация ответов или результатов работы от МАС или ИА;
- выполнение операций по изучению работы информационных структур исследуемых компьютерных сетей.

Оптимальное место расположения третьего уровня – рабочие места пользователей, на которых установлены операционные системы Unix, Windows и т. д., содержащие графический или текстовый интерфейсы для работы с МАС (ИА).

Важным звеном функционирования СУПД на основе МАС является эффективная работа программных средств первого уровня, в основу которого положены основополагающие факторы управления потоком данных.

В основу второго уровня СУПД положены функции объединения всех задействованных систем. К объекту управления потоком данных второго уровня относилась таблица правил системы Firewall операционной системы Unix. Исходя из критериев управления потоком данных относительно протоколов, портов и IP-адресов формировался конфигурационный файл ИА.

МАС состояла из ИА, подсистем репозитория и арбитра ресурсов. При функционировании МАС использовались три типа ИА: агенты данных (D-агенты), агенты управления (C-агенты) и новостные агенты (N-агенты).

Агенты данных составляли важную часть системы и служили основной информационной структурой третьего уровня. Каждому запросу третьего уровня на управление информационными потоками компьютерных сетей соответствовал агент данных второго уровня, которого называли легитимным D-агентом. Также существовали запросы на управление D-агентами, правил управления которыми в таблице системы Firewall не существовало. Такие D-агенты называли нелигитимными. Лигитимные D-агенты создавались немедленно после поступления запроса на управление информационным потоком. Уничтожались они после выполнения необходимых операций. D-агент мог находиться в одном из трех состояний: активном,

пассивном и режиме выполнения операций. Нелигитимные D-агенты создавались в начале запроса пользователя и уничтожались после завершения операции сравнения его идентификационного поля с таблицей системы Firewall.

Лигитимный D-агент характеризовался идентификационным номером и двумя независимыми векторами. Первый вектор (генотип D-агента) являлся набором номеров правил системы Firewall и описания объекта третьего уровня, хранящегося в базе данных/знаний СУПД. Этот вектор характеризовался неизменными для каждого лигитимного D-агента данными.

Второй вектор являлся набором команд возможных операций для С-агента. В общем случае набор второго вектора представлял собой команды системы Firewall на управление трафиком информационными ресурсами компьютерных сетей. Набор второго вектора называли фенотипом D-агента.

Порядок описания D-агента определяла очередность проверки наличия соответствующих правил в таблице системы Firewall. На протяжении своего существования D-агент мог адаптироваться к условиям “существования” с помощью изменения своего фенотипа. Каждому D-агенту также принадлежал список команд системы Firewall для С-агентов, которые были необходимы для управления потоком данных.

Агенты управления (С-агенты) образовывались с помощью программ – клиентов пользователей или специальных команд операционной системы (рис. 2).

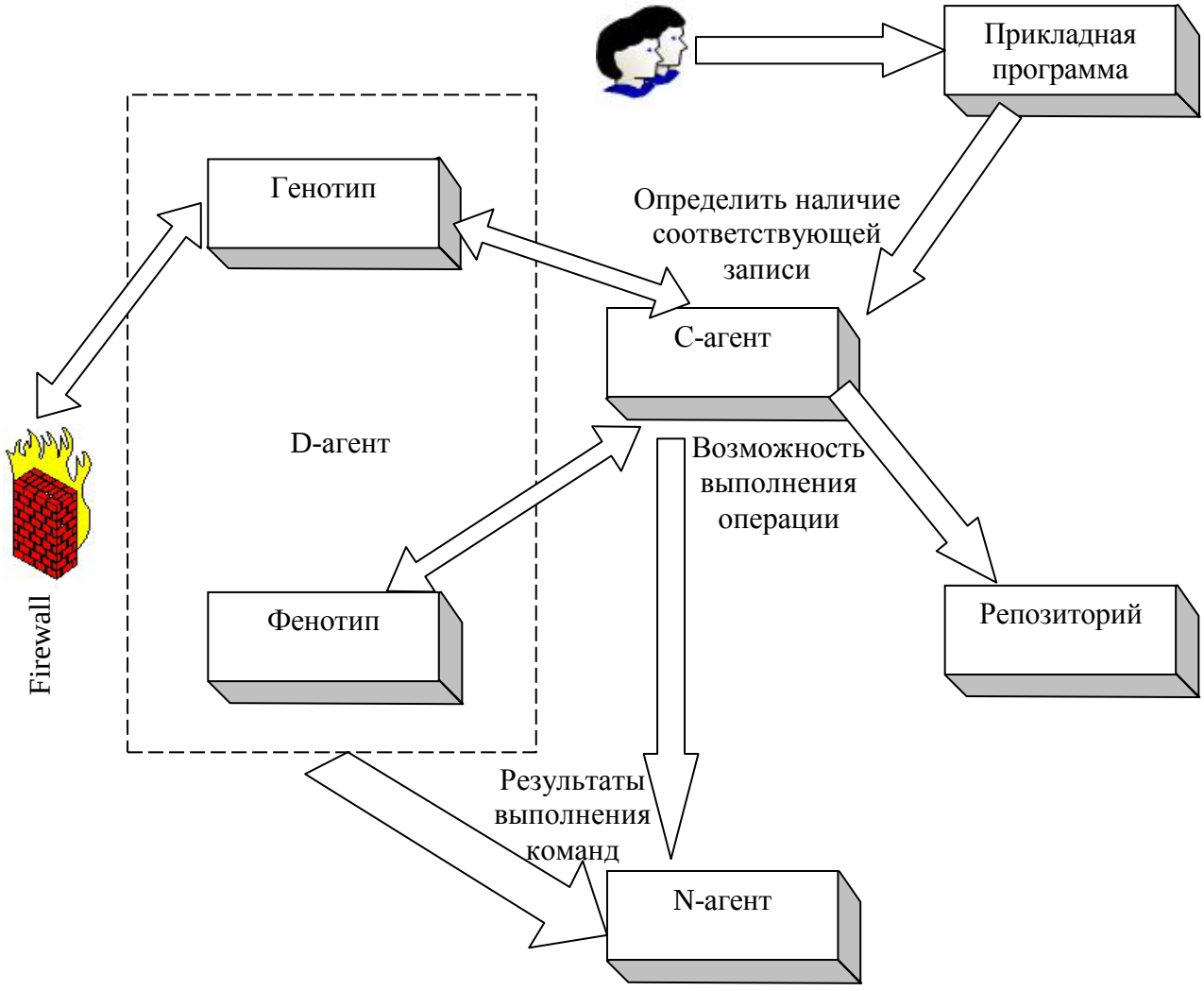

Рисунок 2 – Структура системы управления потоками данных в корпоративной или глобальной компьютерной сети

При выполнении любой команды С-агент создавал сообщение о результате выполнения команды, которое переносилось новостным агентом (N-агент) по адресу назначения. Уничтожались С-агенты после выполнения всех необходимых операций с любыми результатами исходов. В ходе существования С-агентов могли

образовываться несколько новостных агентов, передающих информацию по нескольким адресам. С помощью транспортного протокола TCP/IP они перемещались на заданный узел компьютерной сети, находили соответствующего D-агента и выполняли необходимые операции.

Основным назначением С-агентов являлись:

– поиск соответствующего D-агента с целью выполнения заданной операции по управлению информационными потоками данных в компьютерных сетях;
– создание N-агента, информирующих о результатах выполнения операций.

Новостные агенты обеспечивали интерфейс между МАС (ИА) и программными средствами третьего уровня, в частности, репозиторием. Репозиторий представлял собой базу данных/знаний.

Таким образом, построенная МАС эффективно выполняла функции:

– управления потоком данных в компьютерных сетях;
– защиту информационных ресурсов компьютерных сетей.

IV Выводы

1. В результате использования интеллектуальных технологий, в частности МАС, удается решать комплексные задачи по управлению и защите данных в компьютерных сетях.
2. Процесс защиты информационных ресурсов компьютерных сетей относится к сложным системам управления. Использование методов искусственного интеллекта – мультиагентных систем в области защиты информационных ресурсов является эффективным решением данной проблемы.
3. Наиболее приемлемой и безопасной операционной системой для построения серверной части мультиагентной системы является Unix.
4. В качестве средства управления потоками данных для операционной системы FreeBSD необходимо использовать ipfw.
5. Для разработки клиентских рабочих мест достаточно использовать операционную систему Windows.

Литература: ***1.*** *Wooldridge M., Jennings N., 1995. Intelligent Agents: Theory and Practice //Knowledge Engineering Review No. 10 (2).* ***2.*** *Nwana H. S., 1996. Software Agents: An Overview // Knowledge Engineering Review Vol 11, No 3.* ***3.*** *FIPA, 1998. Ontology Service. FIPA 98 Specification. Part 12. October, 1998 http://www.cset.it/fipa* ***4.*** *А. М. Хошаба, С. В. Юхичук Использование интеллектуальных технологий при построении мультиагентных систем в международной компьютерной сети Интернет // 3 міжнародна конференція "Інтернет – Освіта – Наука – 2002" – жовтень 2002. – Вінниця, ВДТУ. – С. 301 – 306.* ***5.*** *А. М. Хошаба, Войцех О. А. Розробка мультиагентних інтелектуальних систем в міжранодній комп'ютерній мережі Internet // Вісник Житомирського інженерно-технологічного інституту. Спецвипуск. – 2002. — С. 53 – 58.* ***6.*** *А. М. Хошаба, Войцех О. А., Месюра Н. В. Использование мультиагентных интеллектуальных систем в международной компьютерной сети Интернет // 5-та научна конференция "Интернет – среда за нови технологии в информационното общество". – октомври 2002. – Велико Търново. – С. 26 – 34.* ***7.*** *Etzioni, Oren, and Daniel Weld (1994), A Softbot-Based Interface to the Internet. Communications of the ACM, 37, 7, 72 p;79.* ***8.*** *Hayes-Roth, B. (1995). "An Architecture for Adaptive Intelligent Systems," Artificial Intelligence: Special Issue on Agents and Interactivity, 72, 329–365.* ***9.*** *Kautz H., B. Selman, and M. Coen (1994), "Bottom-up Design of Software Agents." Communications of the ACM, 37, 7, 143–146* ***10.*** *Maes, Pattie (1995) ed., Designing Autonomous Agents, Cambridge, MA: MIT Press.* ***11.*** *Mülle, J. P., M. Pischel, and M. Thiel (1995), "Modeling Reactive Behaviour in Vertically Layered Agent Architectures," in Wooldridge and Jennings Eds., Intelligent Agents, Berlin: Springer-Verlag, 261–276.* ***12.*** *Smith D. C., A. Cypher and J. Spohrer (1998), "KidSim: Programming Agents Without a Programming Language," Communications of the ACM, 37, 7, 55–67.* ***13.*** *Song, Hongjun, Stan Franklin and Aregahegn Negatu (1998), "A Fuzzy Subsumption Softbot," Proceedings of the ISCA Int Conf on Intelligent Systems, Reno Nevada.* ***14.*** *Wooldridge, Michael and Nicholas R. Jennings (1997), "Agent Theories, Architectures, and Languages: a Survey," in Wooldridge and Jennings Eds., Intelligent Agents, Berlin: Springer-Verlag, 1–22*

УДК 681.3.06