§2 ТЕХНОЛОГИИ И МЕТОДОЛОГИЯ В СИСТЕМАХ БЕЗОПАСНОСТИ

Ляпустин А. Е.

РАЗРАБОТКА И ИССЛЕДОВАНИЕ МОДЕЛЕЙ И МЕТОДИК КОМПЛЕКСНОЙ ЗАЩИТЫ ГЕТЕРОГЕННЫХ ИНФОРМАЦИОННЫХ ПЛАТФОРМ

Аннотация. *Данная работа предполагает анализ современных подходов к разработке комплексных подходов к защите гетерогенных информационных платформ. Несмотря на перечисленные преимущества подходов, большинство из них направлены на решение определенной задачи, не осуществляя комплексное решение проблемы защиты информации в условиях сложных гетерогенных систем. В работе представлена архитектура гетерогенной информационной системы, выступающей в качестве объекта защиты. Результатом проведенного исследования является формирование концепции создания СЗИ, архитектура которой строится на мультиагентном подходе и ориентируется на гетерогенные ИС. Предлагается модель и методика комплексной защиты гетерогенных информационных платформ, а также рассматривается методика интеллектуального обнаружения угроз. В теоретическом плане полученные в ходе исследования результаты предполагают расширение области использования мультиагентного подхода и осуществление его интеграции с интеллектуальным анализом развития и функционирования информационных систем. Практическая целесообразность полученных результатов связана с возможностью их применения разработчиками информационных систем защиты информации.*

Ключевые слова: *защита информации, обнаружение угроз, интеллектуальные системы ЗИ, гетерогенные информационные платформы, информационная безопасность, агенты обнаружения, средства защиты информации, защита информационных систем, централизованные атаки, Обработка информации.*

Review. *This work presents the analysis of the modern approaches towards development of comprehensive systems for protecting heterogeneous information platforms. Despite the advantages of the reviewed approaches, majority of them are aimed at solving a particular task, rather than a complex solution to the problem of protection of*

DOI: 10.7256/2073–8560.2015.4.15662

information in the environment of sophisticated heterogeneous systems. This article demonstrates the architecture of a heterogeneous information system acting as an object of protection. The result of the conducted research lies in the formation of a concept of creation of an Information Security System, the architecture of which is built upon a multi-agent approach and is oriented towards heterogeneous information systems. The author proposes a model for a comprehensive protection of the heterogeneous information platforms and examines the methodology for intelligent threat detection. The results of this research suggest increasing the area of use of the multi-agent approach and its integration into the intelligent analysis of development and functionality of the information systems.

Keywords: *intelligent systemof information protection , threat detection, information security, heterogeneous information platforms, information safety, detection agents, means of information security, information system protection, centralized attacks, information processing.*

В настоящее время развитие информационных систем (ИС) происходит на фоне интенсивного изменения подходов к их проектированию. Большинство ИС — Web-ресурсы, доступ к которым осуществляется с использованием глобальной сети Internet. Постоянный положительный тренд развертывания широкополосного доступа к Internet, наряду с интенсивным развитием информационных технологий повышают нагрузку на ИС. В условиях развития динамических сервисов поддержка тысяч и даже миллионов одновременных сеансов пользователей для информационной системы — трудновыполнимая задача. С увеличением количества одновременных сеансов задача перерастает в невыполнимую. В связи с этим основным направлением развития ИС на современном этапе является формирование гетерогенных информационных платформ, которым свойственно наличие динамического расширения как в области предоставляемых сервисов, так и в сфере обеспечения доступа для увеличивающегося количества пользователей ИС. В качестве примеров развития ИС на современном этапе следует рассматривать развитие облачных технологий и предоставляемых ими сервисов (PaaS, IaaS, SaaS).

Обеспечение информационной безопасности — одна из основных проблем функционирования гетерогенных информационных платформ. В случае «монолитных» ИС уже разработаны методики по проектированию систем защиты информации (СЗИ), тогда как для гетерогенных информационных платформ в рамках разработанных на сегодняшний день методик проектирования СЗИ содержатся лишь комплексы требований, последовательность этапов, сформулированных на неформальном уровне, в связи с чем программирование их осуществления невозможно в связи с высоким уровнем сложности информационной системы и ее распределенностью в рамках множества вычислительных узлов.

В условиях гетерогенных информационных платформ нельзя спрогнозировать все атаки на гетерогенную ИС, предусмотрев возможные сценарии защиты. В связи с этим методы обеспечения информационной безопасности гетерогенной информационной платформы должны базироваться на применении мультипрограммных комплексов, которые могут осуществлять планирование в условиях сложной среды. Данные комплексы должны включать множество компонентов защиты, имеющих специализацию по различным направлениям решаемых задач, к которым относятся следующие: обнаружение угроз, вторжений и т.д. Комплексы должны осуществлять взаимодействие между собой в рамках обмена информацией для того, чтобы в итоге было принято правильное решение. Также в рамках комплексов должна реализовываться возможность осуществления адаптации к новым видам атак. Данные мультипрограммные комплексы называются интеллектуальными СЗИ.

В настоящее время достаточно много исследований проведено в области интеллектуальных систем защиты информации в сфере ИС и компьютерных сетей. Так, в работах [1–3] выдвигается предложение использовать искусственные нейронные сети для определения вторжений в компьютерные сети. Данный подход предполагает использование свойство обучаемости нейросетей, используемое для детектирова-

DOI: 10.7256/2073–8560.2015.4.15662

ния новых типов атак без добавления сигнатур в базу данных системы обнаружения вторжений (IDS). В данной сфере присутствуют результативные векторы исследований, к которым можно отнести проектирование разных топологий нейронных сетей, использование методов их обучения, алгоритмизацию процессов адаптации нейросетей и т.д. Большинство работ посвящается гибридным подходам к проектированию нейросетей при обнаружении вторжений. Например, в работе [3] автор предлагает одновременно осуществлять использование нескольких различных нейросетей, каждая их которых ориентируется на устранение определенного класса угроз. В процессе консолидации результатов их работы вероятность обнаружения угроз повышается.

Работы [4, 5] содержат предложения по использованию архитектурных принципов биологических иммунных систем как основы формирования адаптивных СЗИ. Данные системы называются искусственными иммунными сетями. В качестве фундаментальной основы данных систем следует рассматривать рефлексию и память, определяющие реакцию на внешнее воздействие и запоминание данной реакции с целью применения в будущем.

Работы [6, 7] содержат рассмотрение одного из перспективных подходов к методам обнаружения вторжений и аномалий, в качестве основы которого рассматриваются системы роевого интеллекта — муравьиные алгоритмы, например. В основе данного метода содержится аналогия с поведением колонии муравьев, в процессе поиска пищи использующих след испаряющихся или усиливаемых феромонов с целью поиска кратчайшего пути к пище. Про ект AntMiner+ является одной из реализаций такого подхода.

В рамках перечисленных подходов невозможно комплексное решение проблемы защиты информации в рамках сложных распределенных ИС, несмотря на то, что отдельные задачи по обеспечению информационной безопасности при реализации данных подходов успешно решаются.

Следует отметить, что гетерогенная информационная платформа имеет вариативное количество логических уровней и узлов. Правильное проектирование количества логических уровней является основой для определения функционала ИС, количество узлов — основой для определения производительности.

При разработке СЗИ применительно к гетерогенной информационной платформе следует учитывать возможность допущений: узлы в рамках гетерогенной ИС существуют в условиях изолированной сети; из внешней сети осуществляется доступ исключительно к узлам входа; конфигурация узлов ИС возможна только из изолированной сети; контроль доступа к изолированной сети осуществляется с использованием средств сторонних систем безопасности (например, с использованием VPN-шлюза); количество адми нистраторов ИС ограничено.

При разработке СЗИ следует обеспечить возможность выявления известных для СЗИ видов атак и угроз безопасности ИС; возможности эвристического обнаружения угроз безопасности в рамках неизвестных или модифицированных видов атак; возможность оповещения администратора об инцидентах безопасности и аномальных событиях в работе ИС; возможность самостоятельного принятия решения, направленного на предупреждение вторжения в ИС в рамках собственной сформированной базы знаний; возможность расширяемости параметров при выявлении новых типов угроз или атак.

Создаваемая СЗИ должна быть некоторым гибридным решением, базирующимся на концепции системы обнаружения угроз (IDS), системы обнаружения аномалий и предупреждения вторжений (IPS).

В качестве примера формирования данной системы можно рассматривать применение мультиагентного подхода к решению практических задач по обеспечению безопасности ИС на базе программно-технологических решений [8]. Заслуживают внимания и разработки российско-английской компании Magenta [9], которая также является разработчиком инструментария для создания мультиагентной системы (МАС).

В качестве существенного шага к формированию МАС стало формирование в 2005 г. международной общественной организации в области мультиагентных систем — FIPA (The Foundation for Intelligent Physical Agents) [10], сформировавшей в настоящее время ряд до-

DOI: 10.7256/2073–8560.2015.4.15662

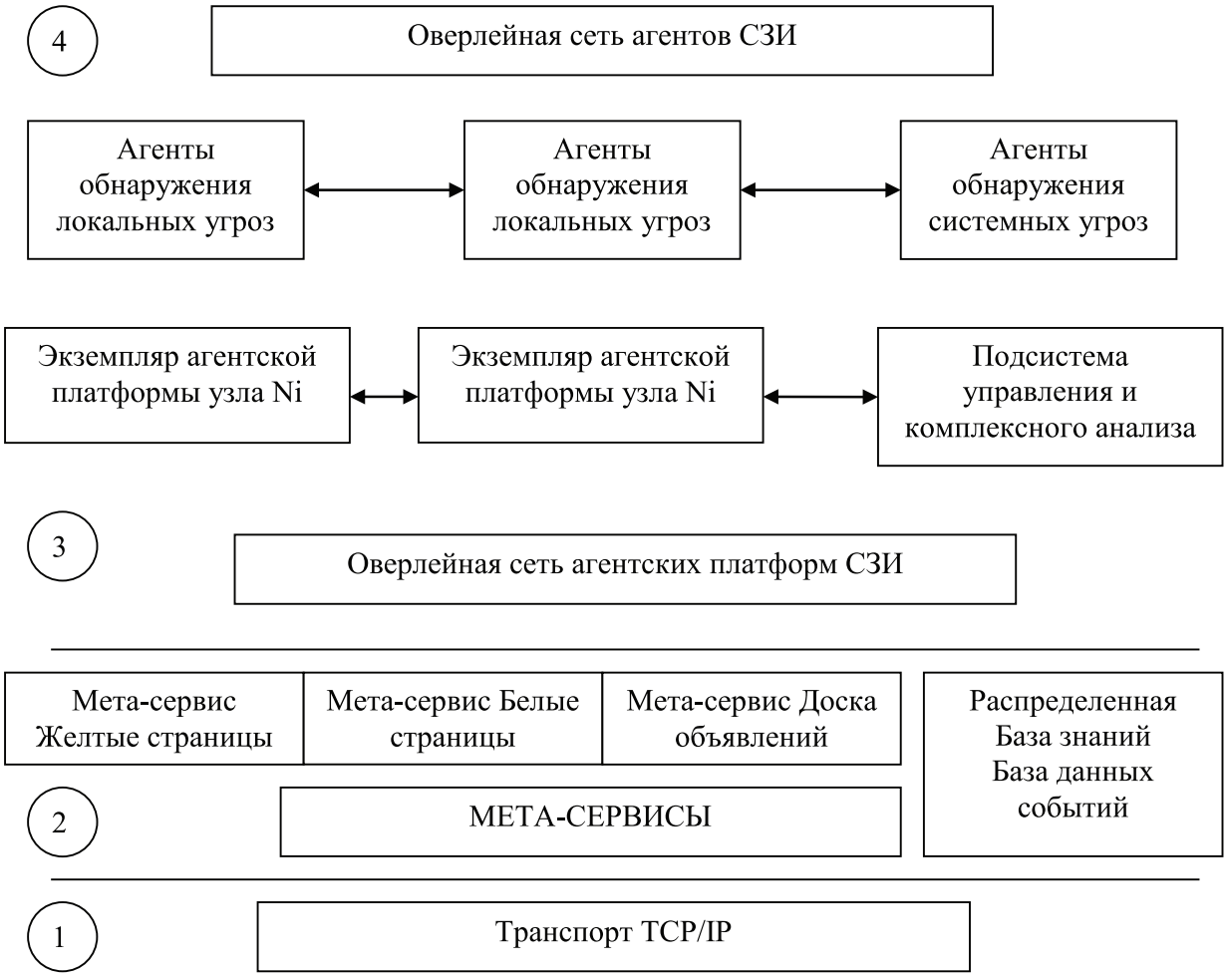

Рис. 1. Общая архитектура СЗИ

кументов и спецификаций, на основе которых происходит разработка МАС.

В основе любой МАС технологическим параметром выступает агентская платформа. Базирование всех имеющихся на сегодняшний день агентских платформ осуществляется на базе использования программной платформы Java — Java Virtual Machine или Java 2 Platform. При осуществлении разработки прикладных программных систем обеспечиваются условия для кроссплатформенности решений. Тем не менее, следует отметить, что при разработке СЗИ данный подход неприемлем, так как выполнение большинства компонентов СЗИ должно осуществляться на низком уровне (на уровне ядра операционной системы, например), чем обеспечивается на основе применения Java Platform.

Данное положение обусловливает необходимость формирования других архитектурных принципов проектирования и разработки СЗИ, основанных на стандартах FIPA с использованием МАС, но имеющих другой подход к реализации в технологическом плане.

Рисунок 1 содержит информацию по формированию общей архитектуры СЗИ, модель которой задается в виде теоретико-множественных отношений:

MSS = {N, MAF, AF, A, MYP, MWP, MBB, EV, RKB}, где N — множество узлов СЗИ; MAF — подсистема управления СЗИ и системного анализа угроз; AF = VAFnode — множество экземпляров агентской платформы; A — множество агентов; MYP — метасервис «желтые страницы»; MWP — мета сервис «белые страницы»; MBB — метасервис «до-

DOI: 10.7256/2073–8560.2015.4.15662

ска объявлений»; EV- множест во зарегистрированных событий в системе; RKB -множество правил базы знаний.

Программно-технологический базис поддержки деятельности агентов СЗИ -собственная агентская платформа, элементы которой следует размещать на каждом узле ИС (VAFnode), каждый узел ИС имеет в качестве соответствия экземпляр агентской платформы.

Агенты обнаружения угроз A = {Al, AS} в мультиагентной СЗИ существуют двух классов (с точки зрения платформ функ ционирования AF и MAF):

- агенты обнаружения локальных угроз узла (AL), функционирование которых осуществляется в рам ках элемента агентской платформы определенного узла ИС, AL е AFnode;
- агенты обнаружения системных угроз (AS), функционирование которых осуществляется в рам ках элемента подсистемы управления и системного анализа угроз, AS е MAFnode.

Функциональная точка зрения предполагает классификацию групп на основе перечня актуальных угроз для ИС (сетевые атаки, несанкционированность доступа и т.д.). Данные группы подразделяются на локальные (относящиеся к одному узлу ИС) и системные (относящиеся к двум и более узлам ИС).

При разработке СЗИ следует учитывать, что по типу мониторинга данная СЗИ выступает в качестве узловой, а по типу архитектуры — гибридной, распределяясь по всем узлам ИС, имеет выделенный узел, связанный с функционированием подсистемы управления и комплексного анализа (MAF). Данная подсистема должна проводить комплексный анализ угроз, осуществлять управление СЗИ, поддержку метасервисов, а также поддержку ряда вспомогательных сервисов.

Следует отметить, что СЗИ не обладает свойством централизованности, несмотря на наличие выделенного узла. Каждый узел предлагаемой СЗИ является самодостаточным при осуществлении локального обнаружения угроз и принятия решений, хотя без центрального узла функциональность СЗИ в целом ограничивается. Может быть сформировано несколько выделенных узлов, но не все из них будут синхронизироваться, что является следствием необходимости обеспечения надежности системы.

На рисунке 1 определяются четыре уровня архитектуры СЗИ. Четвертый — самый верхний — уровень предполагает наличие агентов, обнаруживающих вторжения и аномалии, которые распределены по агентским платформам и по всем узлам ИС, образуя сеть агентов (AON), выступающую в качестве надстройки над сетью агентских платформ — третьим уровнем СИЗ.

Таким образом:

AON = (AF x Al)u (MAF x As).

Следует рассматривать каждый экземпляр агентской платформы (AFnode) в качестве базиса для деятельности агентов. При этом должны реализовываться базовые сервисы, обеспечивающие взаимодействие агентов (сервисы «белых» и «желтых» страниц, доска объявлений). Реализация функций агентской платформы по доступу к СЗИ осуществляется через провайдера. Также должен реализовываться сервис базы знаний, включающей информацию о взаимоотношениях между агентами, о кооперативном поведении агентов, об угрозах безопасности, уровне потенциальных атак и т.д. Каждая область знаний строится на основе соответствующей онтологии.

На базе множества агентских платформ, а также на базе подсистемы управления и осуществления комплексного анализа (MAF) происходит объединение в оверлейную сеть (AON), которая реализует ряд распределенных сервисов, обеспечивающих взаимодействие агентов между собой и осуществляющих функционирование на основе различных агентских платформ. К данным сервисам относятся следующие: «желтые страницы» (MYP) и «белые страницы» (MWP), а также «доска объявлений» (MBB).

Локальные базы знаний агентских платформ, объединяясь, формируют распределенную базу знаний СЗИ и множество правил RKB, что предоставляет возможность использовать накопленные знания в рамках системы агенту, находящемуся в любом узле СЗИ. Зарегистрированные агентами события (EV) хранятся в СУБД, распределение которой может осуществляться по узлам СЗИ или данная СУБД может быть централизованной.

DOI: 10.7256/2073–8560.2015.4.15662

Нижний — первый — уровень абстракции в рамках общей архитектуры СЗИ предполагает наличие транспортной системы взаимодействия в сети между узлами СЗИ, которая базируется на стандартном стеке протоколов TCP/IP.

В качестве основной угрозы для современных гетерогенных информационных платформ следует рассматривать централизованные или распределенные атаки, выполнение которых осуществляется по определенному сценарию В качестве примера таких атак следует рассматривать «отказ в обслуживании» (DoS), атаки на web-сервер или СУБД и т.д.

Любая из вышеприведенных атак оставляет определенную информацию в журналах событий, в данных мониторинга. Совокупность данных по атакам может выступать в качестве паттерна определенного вида атаки как на отдельный узел в рамках ИС, так и на гетерогенную информационную платформу в целом. Для каждой атаки существует свой уникальный паттерн, а также определенное множество паттернов.

Одна из основных задач СЗИ — обнаружение угроз безопасности и определение атак на узлы ИС — должна решаться на стадии инициализации и запуска СЗИ. В рамках методики обнаружения угроз безопасности предполагается, что для каждого узла характерно наличие множества агентов обнаружения угроз, каждый из которых является базовым классификатором атак. При этом для каждого агента характерна специализация на определенного вида атаках, каждый агент обладает информацией о ее паттернах и одним из методов обработки данных с целью определения данных паттернов.

Алгоритмический базис функционирования агентов предполагает использование любых статистических методов обработки информации, включая алгоритмизацию кластеризации, Марковские модели, т.д.

Важно подчеркнуть, что агентов по выявлению конкретного типа атаки (на пример, DDoS) в агентской платформе одновременно функционирует несколько, каждый из которых «обладает» своим алгоритмическим базисом. В рамках своей работы агент осваивает большое количество паттернов, характерных для атак определенного вида, что приводит к повышению вероятности их обнаружения, а также к повышению рейтинга агента в рамках СЗИ.

Основой мотивации агента к саморазвитию является собственный рейтинг, определяющий уровень конкурентного преимущества агента перед другими агентами. Решение задачи обнаружения угроз на основе МАС базируется на наличии цели или мотива, характерных для каждого агента, а также на конкуренции между агентами.

При условии определения агентами наличия атаки на узел менеджер принятия решения использует одну из схем объединения решений агентов, или определение условной вероятности присутствия факта атаки.

Первоначальный этап проектирования СЗИ связан с использованием одного из простых методов — метода простого взвешенного голосования. Данный подход предполагает использование суммы условных вероятностей по каждому из агентов в пользу определенного вида атаки, с осуществлением последующего нормирования их по рейтингу.

В качестве результата используется выявление типа атаки, осуществляемой на ИС. Если в базе знаний узла имеются «знания» по данному классу атаки и ее условная вероятность превосходит некоторое пороговое значение (настраиваемой экспер том), то менеджер принятия решения может самостоятельно принять меры по пресечению данной атаки (посредством эффекторов агентской платформы). Если «знания» по данному типу атаки отсутствуют или условная вероятность выявле ния атаки низкая, то для пресечения потенциальной атаки привлекается адмони стратор-эксперт.

Таким образом, данная работа предполагает анализ современных подходов к разработке комплексных подходов к защите гетерогенных информационных платформ. Несмотря на перечисленные преимущества подходов, большинство из них направлены на решение определенной задачи, не осуществляя комплексное решение проблемы защиты информации в условиях сложных гетерогенных систем.

В работе представлена архитектура гетерогенной информационной системы, выступающей в качестве объекта защиты. Результатом проведенного исследования является формирование концепции создания СЗИ, архитектура

DOI: 10.7256/2073–8560.2015.4.15662

которой строится на мультиагентном подходе и ориентируется на гетерогенные ИС.

В теоретическом плане полученные результаты предполагают расширение области использования мультиагентного подхода и осуществление его интеграции с интеллектуальным анализом развития и функционирования ИС.

Практическая целесообразность полученных результатов связана с возможностью их применения разработчиками ИС защиты информации.

БИБЛИОГРАФИЯ

1. Koch R., Dreo G. Fast Learning Neural Network Intrusion Detection System // Third International Conference on Autonomous Infrastructure, Management and Security (AIMS'2009), The Netherlands, Proceedings.—2009.— P. 187–190.
2. Bitter C., North J., Elizondo D. A., Watson T. An Introduction to the Use of Neural Networks for Network Intrusion Detection // Computational Intelligence for Privacy and Security Studies in Computational Intelligence.—2012.— Vol. 394.— P. 5–24.
3. Поздняков С. А. Использование схемы совпадений в системах обнаружения вторжений на основе нейронных сетей // Вестник Омского университета.—2012.—№ 2.— С.189–190.
4. Абрамов Е. С. Построение адаптивной системы информационной безопасности // Известия ЮФУ. Технические науки.—2009.— С. 99–109.
5. Котенко И. В., Нестерук Ф. Г., Шоров А. В. Концепция адаптивной защиты информационно-телекоммуникационных систем на основе парадигм нервных и нейронных сетей // Труды СПИИРАН.—2012.— Вып. 4(23).— С.100–115.
6. Tsang C.— H. Kwong S. Ant colony clustering and feature extraction for anomaly intrusion detection // Studies in computational intelligence.—2006.— Vol. 34.— P. 101–121.
7. Таран А. А. Приложения алгоритма AntMiner+ к задаче классификации событий при анализе сетевого трафика // Известия ЮФУ. Технические науки.—2012.— Т. 137, № 12.— С. 60–67.
8. http://eprints.agentlink.org/view/type/project.html (дата обращения 18.06.2013).
9. http://www.magenta-technology.ru/ru/ (дата обращения 18.06.2013).
10. http://www.fipa.org/index.html (дата обращения 18.06.2013).

REFERENCES (TRANSLITERATED)

1. Koch R., Dreo G. Fast Learning Neural Network Intrusion Detection System // Third International Conference on Autonomous Infrastructure, Management and Security (AIMS'2009), The Netherlands, Proceedings.—2009.— P. 187–190.
2. Bitter C., North J., Elizondo D. A., Watson T. An Introduction to the Use of Neural Networks for Network Intrusion Detection // Computational Intelligence for Privacy and Security Studies in Computational Intelligence.—2012.— Vol. 394.— P. 5–24.
3. Pozdnyakov S. A. Ispol'zovanie skhemy sovpadenii v sistemakh obnaruzheniya vtorzhenii na osnove neironnykh setei // Vestnik Omskogo universiteta.—2012.—№ 2.— S.189–190.
4. Abramov E. S. Postroenie adaptivnoi sistemy informatsionnoi bezopasnosti // Izvestiya YuFU. Tekhnicheskie nauki.—2009.— S. 99–109.
5. Kotenko I. V., Nesteruk F. G., Shorov A. V. Kontseptsiya adaptivnoi zashchity informatsionno telekommunikatsionnykh sistem na osnove paradigm nervnykh i neironnykh setei // Trudy SPIIRAN.—2012.— Vyp. 4(23).— S.100–115.
6. Tsang C.— H. Kwong S. Ant colony clustering and feature extraction for anomaly intrusion detection // Studies in computational intelligence.—2006.— Vol. 34.— P. 101–121.
7. Taran A. A. Prilozheniya algoritma AntMiner+ k zadache klassifikatsii sobytii pri analize setevogo trafika // Izvestiya YuFU. Tekhnicheskie nauki.—2012.— T. 137, № 12.— S. 60–67.
8. http://eprints.agentlink.org/view/type/project.html (data obrashcheniya 18.06.2013).
9. http://www.magenta-technology.ru/ru/ (data obrashcheniya 18.06.2013).
10. http://www.fipa.org/index.html (data obrashcheniya 18.06.2013).

DOI: 10.7256/2073–8560.2015.4.15662