Информатика, вычислительная техника и управление

УДК 004.7:004.422.8
DOI:

А.В. Птицын, Л.К. Птицына

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ МЕТОДОЛОГИЧЕСКОГО БАЗИСА АГЕНТНЫХ ТЕХНОЛОГИЙ

Представлены ситуационные и технологические основания для развития научных исследований в области информационной безопасности. Выделены концептуальные преимущества агентных технологий для обеспечения информационной безопасности. Описаны целевые ориентиры методологии профилирования качества интеллектуальных агентов. Раскрыт методологический базис агентных технологий. Построены расширенные объектно-ориентированные модели интеллектуальных агентов. Выполнен анализ моделей в условиях априорной неопределённости ситуаций при достижении целей.

Ключевые слова: информационная безопасность, агентные технологии, интеллектуальный агент, профиль качества, методологический базис, расширенная модель, вероятность достижения цели.

A.V. Ptitsyn, L.K. Ptitsyna

ENSURING INFORMATION SECURITY BASED ON METHODOLOGICAL BASIS OF AGENT TECHNOLOGIES

Among great number of characteristic properties of the present day there is emphasized a development of socium technosphere. Particular attention is paid to the use of scientific educational production environment in professional activities. In relation to economy conditions of the information society there are considered objective prerequisites for scientific research development in the field of information security. At the conceptual level there is substantiated an expediency of artificial intelligence active participation in the assurance of information security. As artifacts to ensure information security the intellectual computer agents are chosen. As a supporting basis of agent intelligence there are used algorithms of agent action planning. For the further perfection of computer agents of information security it is offered to use a model-analytical intelligence. The purpose of investigations consists in the development of the intelligence of computer agents to control and fulfill guarantees in the assurance of information security. As a result of the review of scientific achievements on the investigation of intelligent information agents there is chosen a methodological basis of agent technologies. In the context of information security threats appeared there is substantiated a topicality of the analysis of the situation integration of computer agent simultaneous actions to achieve purposes specified. In accordance with the methodology chosen there are developed expended object-directed models of computer agents on information security. With the aid of the method of sub-process free integration the analysis of model formation is carried out. In the course of the analysis there is formed a model-analytical intelligence of computer agents on information security. The computer agent intelligence developed allows overcoming a priori uncertainty regarding guarantees in the assurance of information protectability.

Key words: information security, agent technologies, intelligent agent, quality profile, methodological basis, expended model, likelihood in goal achievement.

Одной из характерных особенностей современности является стремительное развитие техносферы социума. Благодаря этому развитию расширяются области профессиональной деятельности, предусматривающие погружение различных процессов деятельности в научно-образовательно-производственные среды. В условиях экономики информационного общества любая научно-образовательно-производственная среда создаётся и разворачивается на основе информационной инфраструктуры, с которой ассоциируется как обеспечение неоспоримых преимуществ профессиональной деятельности, так и появление потенциальных угроз, способных не только вызвать снижение качества её результатов, но и прервать технологический процесс деятельности, создав при этом условия для проявления

непредсказуемых негативных последствий. В связи с реальным положением дел по погружению различных видов профессиональной деятельности в научно-образовательно-производственные среды образуются объективные предпосылки для развития научных исследований в области информационной безопасности, формирования безопасных информационных технологий и их оперативного внедрения в технологическое сопровождение выполняемых работ.

Целевые обобщения формальных основ научных исследований в области безопасности, как и в любой другой области, осуществляются на методологическом уровне. Каждое целевое обобщение проводится в контексте определённой парадигмы обеспечения информационной безопасности, согласующейся с современными представлениями о состоянии дел в этой области.

По мере развития научно-методических и научно-практических достижений в сфере искусственного интеллекта соответствующие аспекты его функциональности отражаются в содержании выбираемых парадигм обеспечения информационной безопасности.

Обращение внимания на возможность использования искусственного интеллекта в области информационной безопасности является следствием признания объективной необходимости активизации в сопутствующих процессах не только интеллекта разработчиков и проектировщиков научно-образовательно-производственных сред, но и интеллектуальных инфокоммуникационных технологий, включающих соответствующие артефакты.

С позиции деятельного участия артефактов в обеспечении информационной безопасности выделяется направление интеллектуализации, основанное на такой категории, которая концентрируется на создании действующих рационально систем. Указанное направление интеллектуализации разворачивается на базе компьютерных агентных технологий [1]. В указанных технологиях отдельно взятый агент является носителем и выразителем вычислительного, коммуникационного или вычислительно-коммуникационного интеллекта. Подобие рациональных действий компьютерных артефактов действиям профессионалов-субъектов поддерживается с помощью подсистем планирования действий информационных агентов в соответствии с поставленными целями обеспечения информационной защищённости научно-образовательно-производственной среды. Для осуществления подобного рода поддержки предназначаются стратегии и алгоритмы планирования действий интеллектуальных информационных агентов, раскрытые в [2; 3].

Стремление к самооценке эффективности исполнения спланированных действий и прогнозированию успешности достижения поставленных целей воплощается в формировании и подключении к компьютерным агентам их модельно-аналитического интеллекта, предусматривающего определение и вычисление показателей, характеризующих гарантии качества их функционирования. Постепенное развитие формализаций, касающихся формирования модельно-аналитического интеллекта информационных агентов, прослеживается в публикациях [3-8]. В [3] описываются ключевые этапы анализа поведения интеллектуальных информационных агентов в среде информационных сетей при явных схемах описания предусловий выполняемых ими действий. В [4] совершенствуются процедуры анализа моделей поведения интеллектуальных информационных агентов на случай априорной неопределенности в описаниях функций синхронизации выполняемых ими действий. В [5] выполняется систематизация основных достижений по аналитическому моделированию интеллектуальных информационных агентов. В [6] приводятся нововведения, позволяющие учитывать при аналитическом моделировании динамические приоритеты в объединении распределённых действий интеллектуальных информационных агентов. В [7] представляется система формализаций, предназначенная для формирования динамических профилей комплексных систем защиты информации. В [8] предлагается методоло-

гический базис агентных технологий для обеспечения информационной защищённости, ориентированный на генерацию модельно-аналитического интеллекта для мониторинга эффективности исполнения спланированных действий и прогнозирования успешности достижения компьютерными агентами поставленных целей.

Высокая степень абстракции, задействованная при описании методологического базиса агентных технологий для обеспечения информационной защищённости, с одной стороны, не ограничивает масштабы архитектурного многообразия комплексных систем защиты информации, а с другой стороны, требует определённого рода детализации, демонстрирующей конструктивность предлагаемых формализаций, приводящей к определению математического обеспечения подсистемы модельно-аналитического интеллекта информационных агентов. В связи с этим в представляемом исследовании раскрывается содержание процесса определения математического обеспечения подсистемы модельно-аналитического интеллекта компьютерных агентов на основе методологического базиса агентных технологий для обеспечения информационной защищённости.

При разработке математического обеспечения подсистемы модельно-аналитического интеллекта предполагается, что перед интеллектуальным компьютерным агентом информационной безопасности ставится задача достижения цели в крупномасштабной сети. Первичная цель заключается в обнаружении появляющихся угроз, а вторичная - в их отражении.

Согласно [8], ситуация достижения цели в крупномасштабной гетерогенной сети с помощью интеллектуального компьютерного агента информационной безопасности описывается кортежем

$$\mathbf{S}_v = \langle \mathbf{V}, \mathbf{f}^s(\mathbf{k}_0^s), \mathbf{f}^f(\mathbf{k}_0^f), \mathbf{C}, \mathbf{P}_I, \mathbf{F}_A, \mathbf{F}_B, \mathbf{F}_N, \mathbf{F}_O, \mathbf{N}_O \rangle,$$

где $\mathbf{V}$ - вектор отображения цели; $\mathbf{f}^s(\mathbf{k}_0^s)$ - вектор плотностей распределения вероятностей $\mathbf{k}_0^s$ дискретного времени успешного выполнения запросов информационного агента; $\mathbf{f}^f(\mathbf{k}_0^f)$ - вектор плотностей распределения вероятностей $\mathbf{k}_0^f$ дискретного времени неуспешного выполнения запросов информационного агента; $\mathbf{C}$ - матрица инциденций, представляющая вырожденный граф объектно-ориентированной модели параллельных действий информационного агента; $\mathbf{P}_I$ - множество матриц вероятностей переходов, характеризующих последовательные действия в параллельных профилях информационного агента; $\mathbf{F}_A$ - вектор функций объединения последовательно выполняемых действий информационного агента; $\mathbf{F}_B$ - вектор функций разветвления последовательно выполняемых действий информационного агента; $\mathbf{F}_N$ - вектор априорно неопределённых функций объединения распараллеленных действий информационного агента; $\mathbf{F}_O$ - вектор функций распараллеливания действий информационного агента; $\mathbf{N}_O$ - нотация объектно-ориентированного моделирования.

В соответствии с представленным методологическим базисом агентных технологий построим в классе диаграмм деятельности и проанализируем расширенные объектно-ориентированные модели достижимости целей компьютерными агентами информационной безопасности при неизвестных описаниях функциональных спецификаций механизмов синхронизации их распараллеленных действий, сформированных планировщиками.

При моделировании деятельности компьютерных агентов информационной безопасности рассмотрим следующие типовые случаи достижимости целей:

- априорно неопределённый механизм синхронизации подпроцессов параллельного процесса взаимодействия с I реплицированными информационными источниками;
- априорно неопределённый механизм синхронизации подпроцессов параллельного процесса взаимодействия с I нереплицированными информационными источниками.

В параметрическом пространстве расширенных объектно-ориентированных

моделей компьютерного агента информационной безопасности $\mathbf{f}^S(\mathbf{k}_0^S)$ (вектор плотностей распределения вероятностей $\mathbf{k}_0^S$ дискретного времени успешного выполнения его взаимодействия с информационными источниками) представляют плотности распределений дискретных времен $f_1^S(k_{01}^S), f_2^S(k_{02}^S),..., f_I^S(k_{0I}^S)$, а $\mathbf{f}^f(\mathbf{k}_0^f)$ (вектор плотностей распределения вероятностей $\mathbf{k}_0^f$ дискретного времени неуспешного его взаимодействия с информационными источниками) - плотности $f_1^f(k_{01}^f), f_2^f(k_{02}^f),..., f_I^f(k_{0I}^f)$.

Кортеж описания расширенных объектно-ориентированных моделей компьютерного агента информационной безопасности дополняет $\mathbf{F}_B$ - вектор функций разветвления последовательно выполняемых действий, характеризуемый вероятностями $p_1, p_2,..., p_I$ успешного выполнения его взаимодействия с первым, вторым … *I*-м информационным источником соответственно и вероятностями альтернативных событий $(1-p_1),(1-p_2),...,(1-p_I)$.

Согласно методу свободного объединения подпроцессов, для описания характеристик $\mathbf{F}_N$ - вектора априорно неопределённых функций объединения распараллеленных действий компьютерного агента информационной безопасности введем вероятности

$p_{1,1}^{(2)}, p_{2,1}^{(2)},..., p_{I,1}^{(2)}, p_{1,1}^{(3)}, p_{2,1}^{(3)},..., p_{I,1}^{(3)}$, характеризующие события объединения.

Первоначально рассмотрим случай достижимости целей при параллельном взаимодействии с реплицированными информационными источниками.

Пусть $f_0(k_0=0)=1$. В последующем снимем это допущение посредством дополнения системы математических преобразований расширенной объектно-ориентированной модели.

Объектно-ориентированная модель, соответствующая рассматриваемому случаю, приведена на рис. 1.

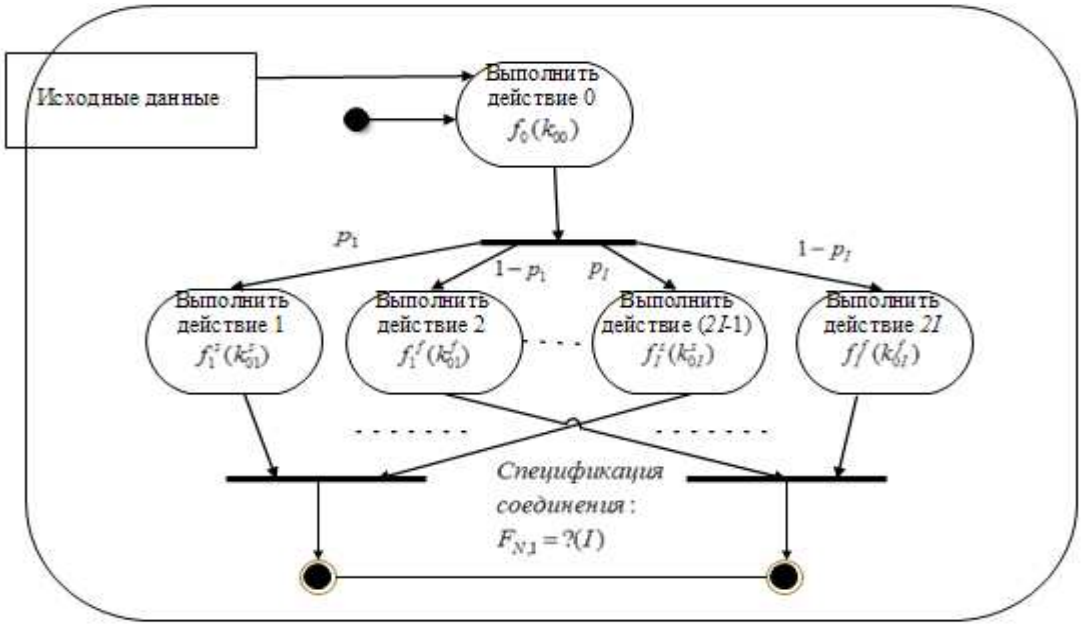

Рис. 1. Диаграмма деятельности компьютерного агента по достижению целей в сети при параллельном взаимодействии с *I* реплицированными информационными источниками при априорно неопределённом механизме синхронизации действий

Согласно методу свободного объединения подпроцессов, построенная модель преобразуется к виду, представленному на рис. 2. Для преобразованной модели справедливы следующие условия:

- для неуспешного выполнения взаимодействия:

$$\mathbf{p^{(2)}} = \left\| \begin{matrix} p_{1,1}^{(2)} \\ p_{2,1}^{(2)} \\ \dots \\ p_{I,1}^{(2)} \end{matrix} \right\| ; \sum_i p_{i,1}^{(2)} = 1 ; \sum_{k_{0i}^f} f_i^{\,f}(k_{0i}^f) = 1 ; \; k_{0i}^f = 1,2,\dots,K_{i\_\max}^f ; \; i = 1,2,\dots,I \; ; \quad (1)$$

- для успешного выполнения взаимодействия:

$$\mathbf{p^{(3)}} = \left\| \begin{matrix} p_{1,1}^{(3)} \\ p_{2,1}^{(3)} \\ \dots \\ p_{I,1}^{(3)} \end{matrix} \right\| ; \sum_i p_{i,1}^{(3)} = 1 ; \sum_{k_{0i}^S} f_i^{\,S}(k_{0i}^S) = 1 ; \; k_{0i}^S = 1,2,\dots,K_{i\_\max}^S ; \; i = 1,2,\dots,I . \quad (2)$$

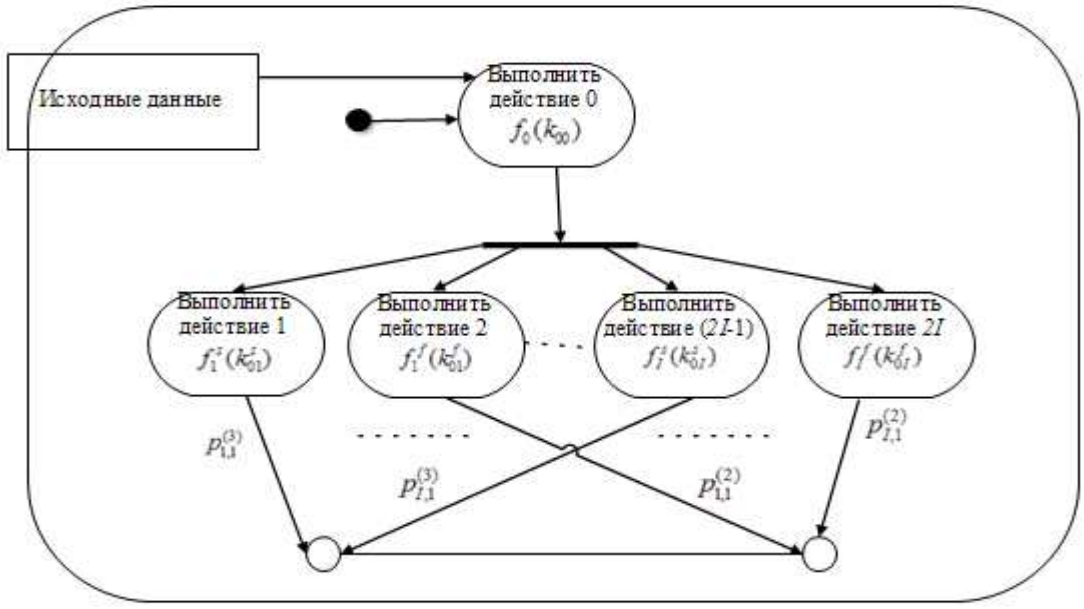

Рис. 2. Диаграмма деятельности компьютерного агента по достижению целей в сети при параллельном взаимодействии с *I* реплицированными информационными источниками при принятии гипотезы о свободном объединении подпроцессов

Представленные вероятности характеризуют ситуационную синхронизацию параллельного взаимодействия интеллектуальных компьютерных агентов с информационными источниками гетерогенных сетей.

Определим $f_{S0}(k_{S0})$ – вероятность дискретного времени успешного достижения цели при условии, что $f_0(k_0 = 0) = 1$:

$$f_{S0}(k_{S0}) = p_1 p_{1,1}^{(3)} f_1^S(k_{01}^S = k_{S0}) + p_2 p_{2,1}^{(3)} f_2^S(k_{02}^S = k_{S0}) + \dots + p_I p_{I,1}^{(3)} f_I^S(k_{0I}^S = k_{S0}), \quad (3)$$

$$k_{S0} = \min_i(\min k_{01}^S, \min k_{02}^S, \dots, \min k_{0I}^S), \dots, \max_i(\max k_{01}^S, \max k_{02}^S, \dots, \max k_{0I}^S). \quad (4)$$

Найдём вероятность дискретного времени неуспешного достижения цели $f_{f0}(k_{f0})$:

$$f_{f0}(k_{f0}) = (1-p_1)p_{1,1}^{(2)} f_1^f(k_{01}^f = k_{f0}) + (1-p_2)p_{2,1}^{(2)} f_2^f(k_{02}^f = k_{f0}) + ... + (1-p_I)p_{I,1}^{(2)} f_I^f(k_{0I}^f = k_{f0}), \quad (5)$$

$$k_{f0} = \min_i(\min k_{01}^f, \min k_{02}^f, ..., \min k_{0I}^f), ..., \max_i(\max k_{01}^f, \max k_{02}^f, ..., \max k_{0I}^f). \quad (6)$$

В том случае, когда k_0 является случайной величиной, $f_S(k_S)$ – вероятность дискретного времени успешного достижения цели определяется соотношением

$$f_S(k_S) = \sum_{k_0} f(k_0) f_{S0}(k_S - k_0), \quad (7)$$

$$k_S = \min(k_0 + k_{S0}), ..., \max(k_0 + k_{S0}), \quad (8)$$

а вероятность дискретного времени неуспешного достижения цели

$$f_f(k_f) = \sum_{k_0} f(k_0) f_{f0}(k_f - k_0), \quad (9)$$

$$k_f = \min(k_0 + k_{f0}), ..., \max(k_0 + k_{f0}). \quad (10)$$

Перейдём к анализу случая достижимости целей в сети при параллельном взаимодействии с I нереплицированными информационными источниками при априорно неопределённом механизме синхронизации действий компьютерного агента.

Расширенная объектно-ориентированная модель, соответствующая такому взаимодействию, изображена на рис. 3.

Преобразованная объектно-ориентированная модель деятельности компьютерного агента по достижению целей в сети при параллельном взаимодействии с I нереплицированными информационными источниками при априорно неопределённом механизме синхронизации действий построена на рис. 4. Преобразование выполнено в соответствии с методом свободного объединения подпроцессов.

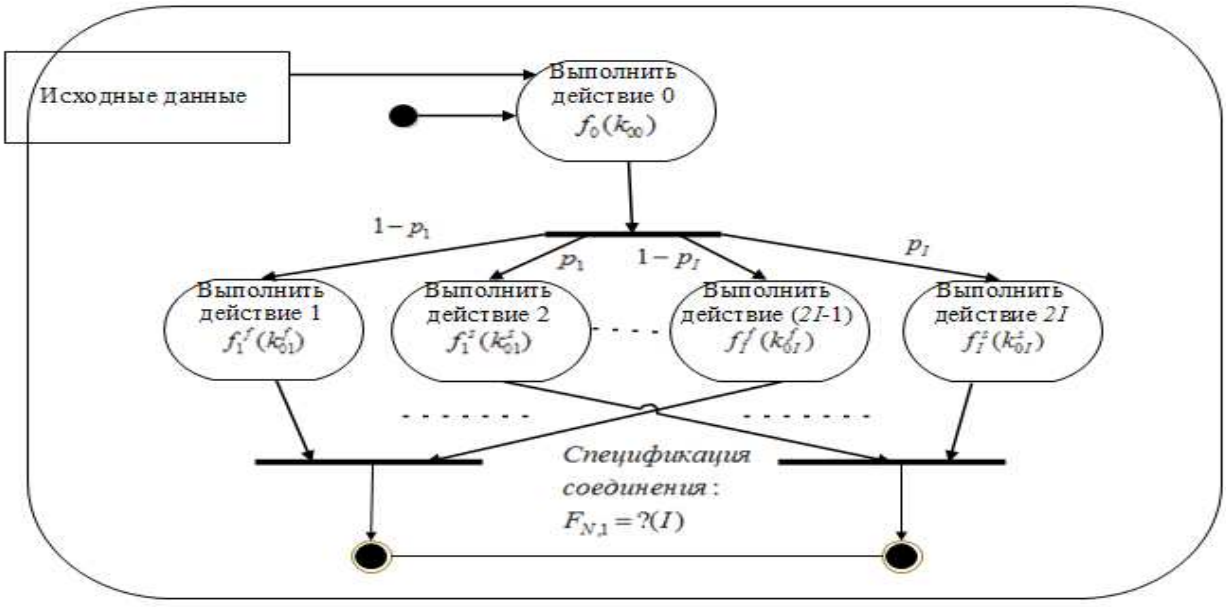

Рис. 3. Диаграмма деятельности компьютерного агента по достижению целей в сети при параллельном взаимодействии с I нереплицированными информационными источниками при априорно неопределённом механизме синхронизации действий

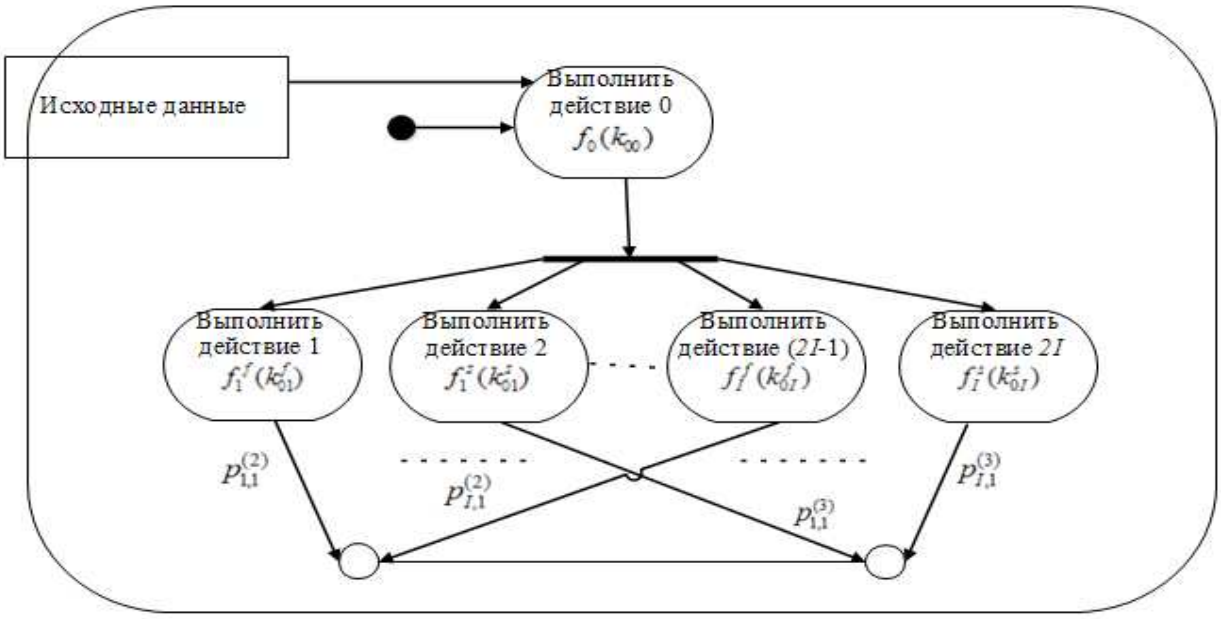

Рис. 4. Диаграмма деятельности компьютерного агента по достижению целей в сети при параллельном взаимодействии с *I* нереплицированными информационными источниками при принятии гипотезы о свободном объединении подпроцессов

Для преобразованной модели (рис. 4) справедливы условия (1) и (2). В соответствии с преобразованной моделью вероятности успешного и неуспешного достижения цели находятся согласно соотношениям (3 - 10).

Далее определим динамические характеристики недостижимости целей при параллельном опросе *I* реплицированных и нереплицированных информационных источников в случае априорно неопределённого механизма синхронизации действий компьютерных агентов информационной безопасности:

- среднее время достижения цели:

$$E\{k_S\} = \sum_{k_S} k_S f_S(k_S); \qquad (11)$$

- среднее время неуспешного достижения цели:

$$E\{k_f\} = \sum_{k_f} k_f f_f(k_f); \qquad (12)$$

- риск срыва временного регламента достижения цели $(1 - P(k_S \le N_{\max}))$ за $N_{\max}$ единиц дискретного времени определяется соотношением

$$(1 - P(k_S \le N_{\max})) = \sum_{k_S > N_{\max}} f_S(k_S). \qquad (13)$$

Выведенные соотношения (3-13) могут входить в состав математического обеспечения модельно-аналитического интеллекта компьютерных агентов информационной безопасности, вводимого в архитектуру для контроля и управления качеством их функционирования.

Разработанный вычислительный интеллект позволяет:

- выявить диапазоны изменения динамических характеристик достижимости целей при использовании интеллектуальных компьютерных агентов информационной безопасности с неизвестными описаниями механизмов синхронизации параллельных действий в зависимости от масштабов сети, планов действий, вероятностных свойств их ситуационного поведения и характеристик информационных источников;
- обосновать требования к архитектуре компьютерных агентов информационной безопасности при установленных требованиях к риску срыва временного регламента достижения целей в условиях ситуационной синхронизации параллельного взаимодействия с информационными источниками гетерогенных сетей.

Новизна приведенных результатов по сравнению с достижениями других исследователей в сфере искусственного интеллекта заключается в формировании расширенных объектно-ориентированных моделей деятельности интеллектуальных компьютерных агентов информационной безопасности, расширении формализаций для определения динамических характеристик достижимости целей в гетерогенных сетях за счет учета вероятностных свойств ситуационной синхронизации параллельного взаимодействия с информационными источниками.

СПИСОК ЛИТЕРАТУРЫ

1. Искусственный интеллект: современный подход: [пер. с англ.] / С. Рассел, П. Норвиг. - 2-е изд. - М.: Вильямс, 2007. - 1408 с.
2. Интеллектуальные технологии и представление знаний. Планирование действий интеллектуальных агентов в информационных сетях: учеб. пособие / Л.К. Птицына, С.В. Добрецов. - СПб. : Изд-во Политехн. ун-та, 2006. - 172 с.
3. Информационные сети. Интеллектуальные информационные агенты: учеб. пособие / Л.К. Птицына, С.М. Шестаков. - СПб. : Изд-во Политехн. ун-та, 2008. - 210с.
4. Разработка и анализ моделей поведения интеллектуальных информационных агентов в гетерогенной сети при априорной неопределенности / Л.К. Птицына, С.Н. Власов // Промышленные АСУ и контроллеры. - М.: Научтехлитиздат, 2011. - № 6. - С. 33-37.
5. Научные достижения в области разработки математического обеспечения интеллектуальных информационных агентов для формирования нового качества высшего политехнического образования: лекция-доклад / Л.К. Птицына, С.Н. Власов // Труды Всероссийской научно-практической конференции с международным участием «Информационные технологии в обеспечении нового качества высшего образования» (г. Москва, 14-15 апр. 2010 г.) / НИТУ «МИСиС». - М.: Исследоват. центр проблем качества подготовки специалистов, 2010. - 52 с.
6. Птицына, Л.К. Информационные технологии проектирования интеллектуальных программных агентов для крупномасштабных сетей / Л.К. Птицына, А.А. Лебедева // Труды Международной научно-методической конференции «Информатизация инженерного образования» - ИНФОРИНО-2014 (г. Москва, 15-16 апр. 2014 г.). - М.: Изд-во МЭИ, 2014. - С. 265-266.
7. 7. Преодоление неопределенности относительно динамических профилей комплексных систем защиты информации / Л.К. Птицына, А.В. Птицын // Вестник Сибирского государственного аэрокосмического университета им. Акад. М.Ф. Решетнева. - Красноярск, 2010. - Вып. 5 (31) (по материалам XII Междунар. симп. по непараметр. методам в кибернетике и системном анализе). - С. 154-156.
8. Птицын, А.В. Методологический базис агентных технологий для обеспечения информационной защищённости / А.В. Птицын // Наукоемкие технологии в космических исследованиях Земли. - 2015. - Т. 7. - № 1. - С. 50-55.

1. *Artificial Intelligence: Current Approach*: [transl. from Engl.] / S. Rassel, P. Norwig. - 2-d ed. - M.: Williams, 2007. – pp. 1408.
2. *Intelligent Technologies and Knowledge Presentation. Planning of Intelligent Agent Actions in Information Networks*: Manual / L.K. Ptitsyna, S.V. Dobretsov. – S-Pb.: Publishing House of Polytechnics, 2006. – pp. 172.
3. *Information Networks. Intelligent Information Agents*: Manual / L.K. Ptitsyna, S.M. Shestakov. – S-Pb. : Publishing House of Polytechnics, 2008. – pp. 210.
4. Development and analysis of behavior models of intelligent information agents in heterogeneous network at a priori uncertainty / L.K. Ptitsyna, S.N. Vlasov // *Industrial ACS and Controllers.* - M.: Nauchtechlitizdat, 2011. - № 6. - pp. 33-37.
5. Scientific achievements in field of mathematical software development of intelligent information agents for higher polytechnic education formation with new quality: lecture-report / L.K. Ptitsyna, S.N. Vlasov // *Proceedings of All-Russian Scientific Practical Conf. with Inter. Participation "Information Technologies in Higher Education Support with New Quality" (Moscow, April14-15, 2010)* / NITU "MIS&A". - M.: Research Center of Quality Problems in Specialist Training, 2010. – pp. 52.
6. Ptitsyna, L.K. Information technologies in intelligent program agent design for large-scale networks / L.K. Ptitsyna, A.A. Lebedeva // *Proceedings of the Inter. Scientific Methodical Conf. "Engineering Education Informatization" - INFORINO-2014* (Moscow, April 15-16, 2014). - M.: Publishing House of MEI, 2014. - pp. 265-266.
7. Uncertainty overcoming regarding dynamic profiles in complex systems of information protection / L.K. Ptitsyna, A.V. Ptitsyn // *Bulletin of Reshetnev Siberian State Aerospace University.* - Krasnoyarsk, 2010. - Ed. 5 (31) (on Proceedings of the XII-th Inter. Symposium on Non-parameter Methods in Cybernetics and System Analysis). - pp. 154-156.
8. Ptitsyn, A.V. Methodological basis of agent technologies to ensure information protectability / A.V. Pritsyn // *Science Intensive Technologies in Space Researches of the Earth.* - 2015. - Vol. 7. - № 1. – pp. 50-55.

Статья поступила в редколлегию 23.01.17.
Рецензент: д.т.н., профессор ПАО «Интелтех»
Мошак Н.Н.

Сведения об авторах:

Птицын Алексей Владимирович, к.т.н., доцент кафедры «Безопасные информационные технологии» Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, e-mail: pticin@inbox.ru.

Птицына Лариса Константиновна, д.т.н., профессор кафедры «Информационные управляющие системы» Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, e-mail: ptitsina_lk@inbox.ru.

Ptitsyn Alexey Vladimirovich, Can. Eng., Assistant Prof. of the Dep. of safety information technologies, Saint-Petersburg National Research University of Information technologies, Mechanics and Optics, e-mail: pticin@inbox.ru.

Ptitsyna Larisa Konstantinovna, D. Eng., Prof. of the Dep. of Information Control Systems, Bonch-Bruevich State Tele-communication University of Saint-Petersburg, e-mail: ptitsina_lk@inbox.ru.