НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
январь–февраль 2019 Том 19 № 1 ISSN 2226-1494 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
January–February 2019 Vol. 19 No 1 ISSN 2226-1494 http://ntv.ifmo.ru/en
УНИВЕРСИТЕТ ИТМО

УДК 004.896

МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОММУНИКАЦИОННЫХ КАНАЛОВ В МУЛЬТИАГЕНТНЫХ РОБОТОТЕХНИЧЕСКИХ СИСТЕМАХ

А.А. Матвеева, Ю.В. Ким, И.И. Викснин

Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация
Адрес для переписки: yulia1344@gmail.com

Информация о статье
Поступила в редакцию 30.05.18, принята к печати
06.11.18 doi: 10.17586/2226-1494-2019-19-1-102-108
Язык статьи – русский

Ссылка для цитирования: Матвеева А.А., Ким Ю.В., Викснин И.И. Методы обеспечения информационной безопасности коммуникационных каналов в мультиагентных робототехнических системах // Научно-технический вестник информационных технологий, механики и оптики. 2019. Т. 19. № 1. С. 102–108. doi: 10.17586/2226-1494-2019-19-1-102-108

Аннотация

Изучена информационная безопасность мультиагентных робототехнических систем. Для исследования выбрана децентрализованная коллективная стратегия группового управления благодаря возможности обеспечения надежного и согласованного взаимодействия агентов посредством общего канала связи. Для корректного и эффективного функционирования группы необходима безопасная передача информации по коммуникационным каналам. Рассмотрены механизмы обеспечения «жесткой» и «мягкой» безопасности в робототехнических системах. Особое внимание уделено сохранению прагматической целостности информации, разработан метод, основанный на теории кредита. Метод подразумевает регламентирование объема передаваемых агентами данных посредством установления фиксированного количества условных единиц информации в единицу времени (рассрочки). В случае удержания агентом данных впоследствии для него снижается объем выплат, принятых к учету, тем самым растет его задолженность. По окончании периода рассрочки вычисляется уровень доверия и репутации агента. При внедрении в группу нового агента рассчитывается кредит, при котором новый агент будет получать информацию от остальных членов группы не в полном объеме, а за вычетом заданной процентной ставки. При этом он должен передавать данные в соответствии с установленными условиями рассрочки. По окончании срока кредита определяется, станет новый агент полноценным членом группы или будет заблокирован. Для оценки эффективности предложенного метода смоделировано взаимодействие группы из десяти агентов. В группу внедрялось два новых агента, один из них являлся диверсантом. Пороговым значением задолженности для принятия агента в группу являлась половина от установленного размера кредита. Реализован ряд независимых опытов, в результате которых диверсант был заблокирован в 90,8 % случаев.

Ключевые слова

децентрализованное коллективное управление, мультиагентные робототехнические системы, теория кредита, прагматическая целостность, информационная безопасность

INFORMATION SECURITY METHODS FOR COMMUNICATION CHANNELS IN MULTIAGENT ROBOTIC SYSTEMS

A.A. Matveeva, I.V. Kim, I.I. Viksnin

ITMO University, Saint Petersburg, 197101, Russian Federation
Corresponding author: yulia1344@gmail.com

Article info
Received 30.05.18, accepted 06.11.18
doi: 10.17586/2226-1494-2019-19-1-102-108
Article in Russian

For citation: Matveeva A.A., Kim I.V., Viksnin I.I. Information security methods for communication channels in multiagent robotic systems. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2019, vol. 19, no. 1, pp. 102–108 (in Russian). doi: 10.17586/2226-1494-2019-19-1-102-108

Abstract

The paper presents the study of multi-agent robotic systems in the context of information security providing. The preference is given to decentralized collective strategy of group management due to secure and consensual agent interaction by common communication channel. For the correct and effective functioning of the robotic group there is a necessity in providing

security of information transfer via communication channels. We consider the mechanisms of “hard” and “soft” security in robotic systems. Special consideration is given to pragmatic information integrity maintenance. To avoid violation occurrence in this integrity category the method based on credit theory was developed. The method implies regulation of information volume transferred by agents through determination of fixed amount for information conventional units per time unit (installment plan). In case of data retention by an agent its payment value is reduced subsequently, thus, its indebtedness is increased. After installment plan period completion agent’s level of trust and reputation is calculated for each agent. When a new agent is incorporated into the group the credit is determined, at which the new agent will get not full information from the other group members but information reduced by the established interest rate. At the same time, this agent must transmit data in accordance with predetermined installment plan conditions. After credit period completion the decision is made whether the new agent is accepted or blocked. To assess the effectiveness of the proposed method the interaction in robotic group consisted of ten agents was modelled. Two new agents were introduced into the group, and one of them was a saboteur. The threshold value of indebtedness for the agent's acceptance to the group is the half of established credit size. Series of independent tests were carried out and the saboteur was blocked in the 90.8 % of them.

Keywords
decentralized collective management, multi-agent robotic systems, credit theory, pragmatic integrity, information security

Введение

За последнее время мультиагентные системы [1, 2] получили широкое распространение. Они помогают автоматизировать такие процессы, как отслеживание посевных комплексов, патрулирование территории с целью выявления фактов нарушения природоохранного режима, проведение хирургических операций, мониторинг чрезвычайных ситуаций, составление карт мест крушения самолетов и восстановление картины происшествия, управление транспортными средствами и др. [3].

Стратегии группового управления агентами делятся на две группы: централизованные и децентрализованные [4]. В свою очередь, централизованное управление бывает единоначальным и иерархическим. В случае централизованного единоначального управления в группе имеется центральное устройство управления (ЦУУ) – командир, на которого возлагаются задачи планирования и контроля действий всех членов группы. Централизованное иерархическое управление заключается в том, что командир управляет рядом подчиненных, каждый из которых, в свою очередь, управляет определенной подгруппой роботов (агентов) из данной группы.

Преимуществом централизованного управления является простота реализации. Однако все системы группового управления, использующие централизованные стратегии, имеют следующие существенные недостатки: низкая отказоустойчивость – выход из строя одного центрального устройства управления приводит к выходу из строя системы в целом либо значительной ее части; длительное время принятия решений – центральный узел управления должен решать сложную задачу оптимизации действий всех членов группы или подгруппы. Этих недостатков лишены группы, применяющие стратегии децентрализованного управления. Отсутствие ЦУУ минимизирует временные затраты на принятие решений, и некорректное функционирование одного или нескольких агентов значительно не повлияет на работоспособность группы.

Стратегия децентрализованного управления может быть коллективной или стайной. При децентрализованном коллективном управлении агенты группы имеют общий канал обмена информацией друг с другом. В случае децентрализованного стайного управления члены группы не имеют канала связи и принимают решения на основе косвенной информации об изменениях окружающей среды, вызванных действиями других роботов.

Предпочтение отдается стратегии коллективного управления, поскольку общий канал связи обеспечивает общение роботов с целью нахождения оптимального алгоритма достижения поставленных целей. Коллективное управление заключается в том, что в группе из n агентов каждый агент группы R_i ($i \in [1; n]$) обладает собственной системой управления C_i, которая отвечает за действия данного агента. Эти системы объединены общим каналом связи. Информация о действиях, выбранных C_i, передается остальным C_j ($j \in [1; n]$, $i \neq j$), и на основании полученных данных агенты оптимизируют свои действия [5].

Механизмы обеспечения информационной безопасности в мультиагентных робототехнических системах

Для корректного и эффективного функционирования группы, подчиняющейся коллективной стратегии управления, необходимо обеспечить безопасность передачи информации по каналу связи. На данный момент в мультиагентных робототехнических системах используются механизмы обеспечения «жесткой» и «мягкой» безопасности [6]. К первому виду относятся шифрование каналов связи с открытым ключом, использование мобильной криптографии, авторизация агентов. Примером обеспечения «мягкой» безопасности является построение модели доверия и репутации к объектам [7]. Однако одна из ее уязвимостей возникает, когда диверсанты (агенты, целенаправленно саботирующие работу группы) составляют половину или большинство группы: тогда они могут выставлять друг другу высокие оценки доверия, дискредитируя при этом остальных агентов. В качестве метода решения

помимо доверия было предложено измерять репутацию агента в течение всего времени взаимодействия.

Однако перечисленные способы ориентированы в основном на сохранение семантической целостности – смысловой составляющей [8, 9]. Следует учитывать: чтобы не подрывать доверие к себе ложной информацией, агенты могут передавать достоверные факты, но не в полном объеме. В таком случае происходит нарушение прагматической целостности [1]. В настоящей работе большое внимание уделено прагматической целостности информации: достоверности и полноте знаний, на основе которых формируется информационное сообщение. Рассматривается возможность группы агентов для мониторинга закрытых помещений и открытых участков. Под мониторингом подразумевается регулярное обследование с целью выявления нестандартных изменений.

Постановка задачи исследования

Имеется группа, состоящая из N агентов: $R=\{r_1, r_2, \ldots, r_N\}$. Каждый агент обладает совокупностью из M свойств: $S^i = \{r_i |\ s_j^i,\ j \in [1; M]\}$, $i \in [1; N]$. В качестве допущения рассматривается гомогенность группы агентов: $\forall r_i, r_j \in R, i \neq j, i, j \in [1; N]$: $S^i = S^j$. Предполагается, что механизмы жесткой безопасности функционируют корректно.

Агенты взаимодействуют в течение времени T. Группа функционирует на территории, состоящей из нескольких равных участков. Агенты проверяют заданные участки в течение равных промежутков (отрезков) времени t, $t \in T$. По окончании проверки агенты обмениваются собранными данными. Информация I_i, которой располагает каждый i-й агент по истечении t_k перед началом процесса обмена, подразделяется на собственную (о собственном техническом состоянии на текущий момент и техническом состоянии всей группы за предыдущий отрезок времени) и приобретенную (об окружающей среде за период $[t_{k-1};t_k]$):

$$I_{o_i} = I_{cts_{[t_{k-1};t_k]_i}} \cup \left(\bigcup_{j=1}^{N} I_{cts_{[t_{k-2};t_{k-1}]_j}} \right), \quad (1)$$

где I_{o_i} – собственная информация i-го агента; $I_{cts_{[t_{k-1};t_k]_i}}$ – информация i-го агента о его техническом состоянии на текущий момент; $I_{cts_{[t_{k-2};t_{k-1}]_j}}$ – информация j-го агента о его техническом состоянии за предыдущий отрезок времени;

$$I_{a_i} = I_{es_{[t_{k-1};t_k]_i}}, \quad (2)$$

где I_{a_i} – приобретенная информация i-го агента; $I_{es_{[t_{k-1};t_k]_i}}$ – информация i-го агента об окружающей среде на текущий момент;

$$I_i = I_{o_i} \cup I_{a_i}. \quad (3)$$

После обмена данными в группе каждый агент имеет в составе приобретенной информации сведения о текущем техническом состоянии остальных членов группы. Структура данных, находящихся в распоряжении у агентов по окончании информационного обмена по результатам проверки участка в период t_k иллюстрируют формулы:

$$I_{o_i} = I_{cts_{[t_{k-1};t_k]_i}} \cup \left(\bigcup_{j=1}^{N} I_{cts_{[t_{k-2};t_{k-1}]_j}} \right), \quad (4)$$

$$I_{a_i} = I_{es_{[t_{k-1};t_k]_i}} \cup \left(\left(\bigcup_{j=1}^{N, i \neq j} I_{es_{[t_{k-1};t_k]_j}} \right) \cup \left(\bigcup_{j=1}^{N} I_{cts_{[t_{k-1};t_k]_j}} \right) \right), \quad (5)$$

$$I_i = I_{o_i} \cup I_{a_i}. \quad (6)$$

Таким образом, необходимо стремиться к тому, чтобы информация, полученная путем объединения данных, переданных всеми агентами, полностью отражала состояние группы и окружающей среды:

$$I = \bigcup_{i \in [1;n]} I_i, \quad (7)$$

$$I \to U, \quad (8)$$

где U – полная информация о группе и окружающей среде на текущий момент.

Однако в группе могут присутствовать диверсанты, преследующие цель саботировать работу всех ее членов. Чтобы не портить репутацию ложными передаваемыми данными, диверсант может удерживать часть информации, при этом получая в полном объеме сведения от других агентов. Тем самым диверсант препятствует составлению полной картины о группе и окружающей среде и может замедлить продуктивность работы всей группы. Диверсанты могут удерживать информацию от других агентов о:

а) своем техническом состоянии в случае незначительных неполадок;

б) состоянии окружающей среды;

в) своем техническом состоянии и состоянии окружающей среды.

На момент окончания процесса обмена данными в группе за период t_k случаи (а) и (б) описываются формулами:

$$I_{cts_d} \in \tilde{I}_{a_i} < I_{cts_i} \in I_{a_d}, \quad (9)$$

где I_{cts_d} – информация о текущем техническом состоянии диверсанта; $d \in [1; N]$, I_{cts_i} – информация о текущем техническом состоянии i-го проверенного агента; $i \neq d$, $\tilde{I}_{a_i}$ – приобретенная информация i-го агента при деструктивном информационном воздействии диверсанта;

$$I_{es_{[t_{k-1};t_k]_d}} \in \tilde{I}_{a_i} < I_{es_{[t_{k-1};t_k]_i}} \in I_{a_d}, \quad (10)$$

где $I_{es_{[t_{k-1};t_k]_d}}$ – информация о текущем состоянии окружающей среды, переданная диверсантом, $d \in [1; N]$; $I_{es_{[t_{k-1};t_k]_i}}$ – информация о текущем состоянии окружающей среды, переданная i-м проверенным агентом, $i \neq d$.

Случай (в) является обобщающим:

$$\tilde{I}_{a_i} < I_{a_d}, i \neq d. \quad (11)$$

Таким образом, диверсанты влияют на формирование у других агентов I_a:

$$\tilde{I}_{a_i} < I_d \setminus I_{o_d}, i \neq d. \quad (12)$$

Задача исследования состоит в поиске эффективных методов минимизации риска деструктивного информационного воздействия на группу со стороны диверсантов и сохранения прагматической целостности передаваемой информации: $\forall i \in [1; N]\ \tilde{I}_{a_i} = I_{a_i} + \varepsilon$, при этом $\varepsilon \to 0$, $I \to U$.

Обеспечение прагматической целостности передаваемой информации посредством теории кредита

Для вычисления доверия и репутации предлагается способ, основанный на теории кредита. Под кредитом [10, 11] зачастую понимают доверие, которое кредитор оказывает должнику при выдаче ссуды, такое определение удобно адаптировать к механизму обеспечения «мягкой» безопасности. Капиталотворческая теория кредита [12, 13] гласит, что кредитование способствует росту благосостояния населения. В контексте информационной безопасности кредит ведет к повышению защищенности передаваемых в группе данных.

На срок P (полный срок кредита) заемщику выдается кредит на сумму D с определенной годовой процентной ставкой p. По окончании срока заемщик с учетом процентов должен выплатить сумму, равную θ. В течение полного срока кредита по истечении определенных равных отрезков L времени заемщик обязан осуществить фиксированный аннуитетный платеж A, который состоит из тела кредита и процента по займу. При сохранении фиксированного размера аннуитетного платежа пропорции данных двух категорий могут изменяться. Размер аннуитетного платежа рассчитывается по формуле:

$$A = KD, \quad (13)$$

где K – коэффициент аннуитета:

$$K = \frac{h(1+h)^L}{(1+h)^L - 1}, \quad (14)$$

где $h = p/12$.

Таким образом, итоги по выплатам могут быть выражены формулой:

$$\sum_{l=1}^{L} A_l = \theta. \quad (15)$$

В процессе взаимодействия группы агентов предлагается ввести понятия: «рассрочка» и «кредит».

Время взаимодействия T делится на L периодов рассрочки заданной длины. За период рассрочки t_l, $l \in [1;L]$ каждый агент должен передать фиксированный объем информации I. В свою очередь, период взаимодействия t_l разбивается на F равных временных отрезков t_f^l, и по истечении каждого из них все агенты должны передать I/F информации:

$$\sum_{f=1}^{F} v_f^l = I, l \in T. \quad (16)$$

Если агент удержит какую-либо информацию, он нарушит установленный фиксированный объем платежа, и в качестве санкции накладывается штраф, снижающий для этого агента объем выплат,

принятых к учету. Таким образом, у агента появляются задолженности. По окончании рассрочки подсчитываются задолженности каждого агента, и агенты с большим долгом будут иметь меньший показатель доверия, а следовательно, репутации [14]. Проверка выплат будет осуществляться в группе регулярно переизбираемым случайным образом ответственным агентом. Уровень доверия и уровень репутации агента в группе представлены зависимостями:

$$\text{Trust}_i = f\left(\sum_{f=1}^{F} v_f^{l+}\right), L \in T \tag{17}$$

$$\text{Reputation}_i = f\left(\sum_{l=1}^{L}\sum_{f=1}^{F} v_f^{l+}\right), L \in T\,. \tag{18}$$

При внедрении нового агента в момент t_0 необходимо произвести его кредитование на объем переданной информации. Процесс кредитования состоит из следующих шагов:

– планирование периода взаимодействия T нового агента и группы;
– расчет полного срока кредита: $t < P < T$;
– определение начального размера процентной ставки p;
– расчет размера рассрочки v за период P.

В течение P внедренный агент должен передавать фиксированный объем информации, определенный условиями рассрочки, при этом от других агентов он будет получать информацию о группе и окружающей среде с учетом вычета заданного процента. Таким образом, в период выплаты кредита за отрезок времени t_k после обмена информацией с другими агентами приобретенная j-м внедренным агентом информация будет выражаться формулой:

$$I_{a_j} = I_{es_{[t_{k-1};t_k]_j}} \cup (1-p)\left(\bigcup_{j=1}^{N, i\neq j}\left(I_{es_{[t_{k-1};t_k]_j}} \cup I_{cts_{[t_{k-1};t_k]_j}}\right)\right). \tag{19}$$

В процессе взаимодействия процентная ставка будет уменьшаться на определенную величину, в конце полного срока кредита она достигнет нуля. По истечении полного срока кредита проверенный агент становится полноправным членом группы, обновляет условия рассрочки, получает от других членов информацию в полном объеме и может стать ответственным агентом группы для проверки платежей.

Проверка внедренных агентов:

1) сравнение заданного v_{must} и фактически полученного v_{got} по окончании P;
2) сравнение $v_{f_{\text{must}}}$ и $v_{f_{\text{got}}}$ по окончании t_f^l, $f \in [1;F]$, $l \in [1; L]$;
3) подсчет количества несоответствий $v_{f_{\text{must}}}$ и $v_{f_{\text{got}}}$, $f \in [1; F]$, по окончании P.

Решение о блокировании или принятии нового агента группы принимается ответственным агентом.

Предложенный способ обеспечения прагматической целостности информации снижает риск деструктивного информационного воздействия на группу. Диверсантам невыгодно внедряться в группу с высокой процентной ставкой, большим сроком кредита и коротким периодом рассрочки: большое количество проверок не дает возможности удерживать много информации, а расходы (энергетические, временные, информационные) во время кредита превышают доходы, которые могут быть получены после его погашения. Пример данной ситуации иллюстрируют рис. 1 и формула

$$I_{(t_0;P)_{\text{sent}}} > I_{(P;t_{w+1})_{\text{got}}}, w \in [1; L-1], \tag{20}$$

где $I_{(t_0;P)_{\text{sent}}}$ – информация, переданная за период кредита; $I_{(P;t_{w+1})_{\text{got}}}$ – информация, полученная по окончании кредита в следующий период рассрочки.

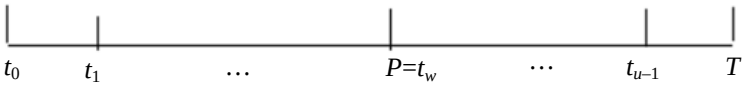

Рис. 1. Временная шкала взаимодействия с группой внедренного агента

Эксперимент

Предложенный способ сохранения прагматической целостности информации был протестирован на специально запрограммированном симуляторе. Начальные условия эксперимента:

– имеется группа из 10 проверенных агентов;
– проверяемая заданной группой агентов территория состоит из 20 равных участков;
– за одну условную единицу времени группа проверяет один участок;
– период рассрочки равен двум условным единицам времени;

- за одну условную единицу времени каждый агент должен передать 10 условных единиц информации;
- в группу внедряют два новых агента: один из них диверсант;
- срок кредита составляет 10 условных единиц времени;
- начальная ставка процента 50 %; по истечении каждого периода рассрочки данная ставка уменьшается на 10 %;
- предельный размер задолженности, при котором новый агент становится полноправным членом группы – половина от заданной суммы кредита;
- диверсанты в зависимости от ситуации могут передавать данные в полном объеме, либо удерживать часть информации.

Был проведен ряд опытов. Распределение размеров задолженностей диверсанта на протяжении эксперимента представлено на рис. 2.

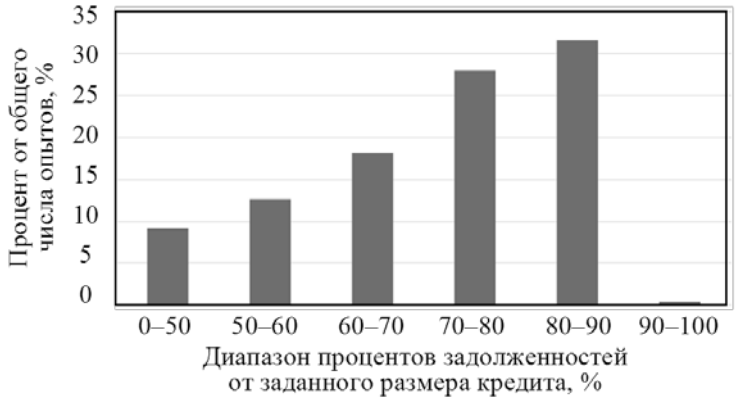

Рис. 2. Распределение размеров задолженностей диверсанта на протяжении эксперимента

На рис. 2 видно, что в результате эксперимента диверсанты корректно определены, так как общее число опытов, в которых задолженность менее 50 %, составляет 9,2 %. В большинстве проведенных симуляций задолженность составила 70–90 %. Таким образом, предложенный подход позволяет обнаруживать диверсантов, нарушающих доступность информации в группе, что приводит к нарушению прагматической целостности информации.

Заключение

Таким образом, задача исследования выполнена. С помощью метода, основанного на теории кредита, возможно минимизировать деструктивное информационное воздействие агентов-диверсантов на группу и обеспечить прагматическую целостность передаваемых данных. Кредитование информации делает невыгодным для диверсантов саботирование работы группы, поскольку требует от них энергетических, временных, информационных затрат.

Литература

1. Комаров И.И., Дранник А.Л., Юрьева Р.А. Моделирование проблем информационной безопасности мультиагентных систем // В мире научных открытий. 2014. № 4 (52). С. 61–70.
2. Ramchurn S.D., Huynh D., Jennings N.R. Trust in multi-agent systems // Knowledge Engineering Review. 2004. V. 19. N 1. P. 1–25. doi: 10.1017/S0269888904000116
3. Шуть В.Н. Мультиагентное управление движением транспортных средств в улично-дорожной сети города // Искусственный интеллект. 2014. № 4. С. 123–128.
4. Ландсберг С.Е., Хованских А.А. Подход к построению мультиагентных систем поддержки принятия решений на основе многоуровневой иерархической эшелонированной архитектуры с частично децентрализованным управлением // Вестник Воронежского государственного технического университета. 2014. Т. 10. № 5. С. 53–55.
5. Каляев И.А., Гайдук А.Р., Капустян С.Г. Модели и алгоритмы коллективного управления в группах роботов. М.: Физматлит, 2009. 280 с.
6. Зикратов И.А., Зикратова Т.В., Лебедев И.С., Гуртов А.В. Построение модели доверия и репутации к объектам мультиагентных робототехнических систем с децентрализованным управлением // Научно-технический вестник информационных технологий, механики и

References

1. Komarov I.I., Drannik A.L., Yurieva R.A. Multiagent information security problem's simulation. *V Mire Nauchnykh Otkrytii*, 2014, no. 4, pp. 61–70. (in Russian)
2. Ramchurn S.D., Huynh D., Jennings N.R. Trust in multi-agent systems. *Knowledge Engineering Review*, 2004, vol. 19, no. 1, pp. 1–25. doi: 10.1017/S0269888904000116
3. Shuts V.N. Multiagent motion control vehicles in the road network of the city. *Iskusstvennyi Intellekt*, 2014, no. 4, pp. 123–128. (in Russian)
4. Landsberg S.E., Khovanskikh A.A. Approach to building multiagent systems support decision based on multilevel hierarchical layered architecture with partially decentralized control. *Bulletin of Voronezh State Technical University*, 2014, vol. 10, no. 5, pp. 53–55. (in Russian)
5. Kalyaev I.A., Gaiduk A.R., Kapustyan S.G. *Models and Algorithms of the Collective Control of Robots Group*. Moscow, Fizmatlit Publ., 2009, 280 p. (in Russian)
6. Zikratov I.A., Zikratova T.V., Lebedev I.S., Gurtov A.V. Trust and reputation model design for objects of multi-agent robotics systems with decentralized control. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2014, no. 3, pp. 30–38. (in Russian)
7. Beshta A.A., Kirpo M.A. Construction of object trust model in the automated information system for preventing destructive

оптики. 2014. № 3 (91). С. 30–38.
7. Бешта А.А., Кирпо М.А. Построение модели доверия к объектам автоматизированной информационной системы для предотвращения деструктивных воздействий на систему // Известия Томского политехнического университета. 2013. Т. 322. № 5. С. 104–108.
8. Jovanov I., Pajic M. Sporadic data integrity for secure state estimation // Proc. IEEE 56th Annual Conference on Decision and Control. Melbourne, Australia, 2017. P. 163–169. doi: 10.1109/cdc.2017.8263660
9. Santra P., Roy A., Majumder K. A Comparative analysis of cloud forensic techniques in IaaS // Advances in Intelligent Systems and Computing. 2017. V. 554. P. 207–215. doi: 10.1007/978-981-10-3773-3_20
10. Лаврушин О.И. Базовые основы теории кредита и его использование в современной экономике // Journal of Economic Regulation. 2017. Т. 8. № 2. С. 6–15. doi: 10.17835/2078-5429.2017.8.2.006-015
11. Евтух А.Т. Теория кредита: социально-экономический аспект // Финансы и кредит. 2005. № 25 (193). С. 21–27.
12. Гурнакова Л.Н. Сущность, теоретические основы понятия «Кредитный рынок» // Проблемы современной экономики. 2011. № 2. С. 83–85.
13. Костерина Т.М., Панова Т.А. Методологические основы анализа границ кредита // Финансы и кредит. 2015. Т. 21. № 32 (656). С. 26–38.
14. Гатауллин Р.И., Назыров М.В., Викснин И.И. Анализ защищенности алгоритмов, базирующихся на коэффициентах доверия и репутации // Сборник трудов V Всероссийского конгресса молодых ученых. Санкт-Петербург, 2016. С. 109–112.

influence on the system. *Bulletin of the Tomsk Polytechnic University*, 2013, vol. 322, no. 5, pp. 104–108. (in Russian)
8. Jovanov I., Pajic M. Sporadic data integrity for secure state estimation. *Proc. IEEE 56th Annual Conference on Decision and Control*. Melbourne, Australia, 2017, pp. 163–169. doi: 10.1109/cdc.2017.8263660
9. Santra P., Roy A., Majumder K. A Comparative analysis of cloud forensic techniques in IaaS. *Advances in Intelligent Systems and Computing*, 2017, vol. 554, pp. 207–215. doi: 10.1007/978-981-10-3773-3_20
10. Lavrushin O.I. The theory of the credit basis and its use in modern economy. *Journal of Economic Regulation*, 2017, vol. 8, no. 2, pp. 6–15. (in Russian)
11. Evtuh A.T. Credit theory: socio-economic aspect. *Finance and Credit*, 2005, no. 25, pp. 21–27. (in Russian)
12. Gurnakova L.N. Essence and theoretical foundations of the credit market concept. Problems of Modern Economics, 2011, no. 2, pp. 83–85. (in Russian)
13. Kosterina T.M., Panova T.A. Methodological bases of the credit limit analysis. *Finance and Credit*, 2015, vol. 21, no. 32, pp. 26–38. (in Russian)
14. Gataullin R.I., Nazyrov M.V., Viksnin I.I. Algorithms security analysis based on confidence and reputation ratios. *Proc. V All-Russian Congress of Young Scientists*. St. Petersburg, 2016, pp. 109–112. (in Russian)

Авторы

Матвеева Анастасия Андреевна – инженер, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, ORCID ID: 0000-0002-2935-991X, anastasiamatveevaitmo@gmail.com

Ким Юлия Вячеславовна – инженер, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, ORCID ID: 0000-0002-6951-1875, yulia1344@gmail.com

Викснин Илья Игоревич – аспирант, научный сотрудник, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, Scopus ID: 57191359693, ORCID ID: 0000-0002-3071-6937, wixnin@mail.ru

Authors

Anastasia A. Matveeva – engineer, ITMO University, Saint Petersburg, 197101, Russian Federation, ORCID ID: 0000-0002-2935-991X, anastasiamatveevaitmo@gmail.com

Yulia V. Kim – engineer, ITMO University, Saint Petersburg, 197101, Russian Federation, ORCID ID: 0000-0002-6951-1875, yulia1344@gmail.com

Ilia I. Viksnin – postgraduate, scientific researcher, ITMO University, Saint Petersburg, 197101, Russian Federation, Scopus ID: 57191359693, ORCID ID: 0000-0002-3071-6937, wixnin@mail.ru