УДК 004.75

**Мухін В.Є.**, д.т.н.; **Ткач М.М.**, к.т.н.; **Корнага Я.І.**, к.т.н.;
**Мостовий Є.О.**, аспірант; **Герасименко О.Ю.**, аспірант

# СТРУКТУРНА МОДЕЛЬ ІНТЕЛЕКТУАЛЬНОГО АГЕНТА ДЛЯ ПІДТРИМКИ ЗАХИЩЕНОЇ ОБРОБКИ ДАНИХ В ГЕТЕРОГЕННИХ РОЗПОДІЛЕНИХ СИСТЕМАХ

**Mukhin V.E., Tkach M.M., Kornaga Ya.I., Mostovoy E.O., Gerasimenko O.Yu. Structural model of intelligent agent to support the data security in the heterogeneous distributed systems.** The growing volume of the processed data in the heterogeneous distributed systems causes the need for a mechanism to support the security of the data processing. In the paper is described the analysis of the intelligent agents using for the data processing and the specifics of the data processing by various criteria. There are presented the main types of intelligent agents and they interaction in the context of unification with different access models, and the structure of the distributed systems with different access models combination in a single system with appropriate levels of access. This structure allows for user to process data from heterogeneous distributed systems. There is suggested the structural model of the intellectual security agent, which supports the constant control over the data access in the heterogeneous distributed information systems. The experimental researches to determine errors of I and II types is performed, and the researches proved that an increase in the number of requests leads to decrease the errors percentages.

***Keywords:*** heterogeneous distributed systems, secure data processing, intelligent agent

**Мухін В.Є., Ткач М.М., Корнага Я.І., Мостовий Є.О., Герасименко О.Ю. Структурна модель інтелектуального агента для підтримки захищеної обробки даних в гетерогенних розподілених системах.** В статті проведено аналіз можливості застосування інтелектуальних агентів до обробки даних та визначено особливості обробки даних за різними критеріями. Запропоновано структуру об'єднання розподілених систем з різними моделями доступу в єдину систему. Розроблено структурну модель інтелектуального агента захисту для постійного контролю дій суб'єктів в гетерогенних розподілених інформаційних системах. Проведено експериментальні дослідження, щодо визначення помилок І та ІІ роду, які довели, що при збільшенні кількості звернень до даних процент помилок зменшується.

***Ключові слова:*** гетерогенні розподілені системи, захищена обробка даних, інтелектуальний агент

**Мухин В.Е., Ткач М.М., Корнага Я.И., Мостовой Е.А., Герасименко О.Ю. Структурная модель интеллектуального агента для поддержки защищенной обработки данных в гетерогенных распределенных системах.** В статье проведен анализ возможности применения интеллектуальных агентов для обработки данных и определены особенности обработки данных по различным критериям. Предложена структура объединения распределенных систем с различными моделями доступа в единую систему. Разработана структурная модель интеллектуального агента защиты для постоянного контроля действий субъектов в гетерогенных распределенных информационных системах. Проведены экспериментальные исследования для определения ошибок I и II рода, которые доказали, что при увеличении количества обращений к данным процент ошибок уменьшается.

***Ключевые слова:*** гетерогенные распределенные системы, защищенная обработка данных, интеллектуальный агент

## Вступ

В зв'язку з стрімким розвитком інформаційних та мережевих технологій постійно зростає необхідність в збільшенні обчислювальних потужностей. Однією з можливостей досягнення цієї мети є використання розподілених систем (РС) обробки даних. В розподілених системах визначається набір незалежних комп'ютерів, що представляється кінцевому користувачеві єдиною системою, тому випливають два основні моменти: першим аспектом такої системи є те, що всі машини автономні, а другим – розподілена система приховує складність та гетерогенну природу апаратного забезпечення, на базі якого вона побудована. Незважаючи на всі переваги таких систем, питання збереження та цілісності даних все одно залишається відкритим [1-3]. Так як дані розподіляються між машинами в

мережі існує потреба в збереженні контролю доступу та обмеження виконання операцій над ними [2-4].

В статті необхідно розробити нові підходи виявлення вторгнень до гетерогенних розподілених систем, які б дозволили ефективніше виявляти загрози несанкціонованого доступу та самостійно навчатись на основі виявлених атак.

**1. Аналіз застосування інтелектуальних агентів в розподілених системах обробки даних**

Розподілені системи створюються для вирішення конкретного типу задач. В зв'язку з великою кількістю вимог до функціональності існує багато різновидів таких систем. На сьогоднішній день можна виділити наступні класифікації РС [4-8]:

1. За способом адміністрування та розміром:
   a. Кластер - відносно невелика кількість комп'ютерів (десятки), об'єднаних в локальну мережу.
   b. Розподілена система корпоративного рівня – сотні ОЕМ, при роботі яких необхідно встановлювати правила сумісного використання ресурсів. Як правило для таких систем можна стандартні підходи адміністрування для організації роботи ресурсів та користувачів.
   c. Grid система – велика кількість комп'ютерів об'єднаних глобальною мережею.
2. За типом задач, під вирішення яких РС створені:
   a. Обчислювальні системи (Computional Grid) – системи, в яких основним обчислювальним ресурсом є потужність процесора.
   b. Інформаційні системи (Data Grid) – тип систем, в яких основним ресурсом є об'єм пам'яті. Такі системи, як правило, використовуються для збереження масивів даних.

В роботі розглянуто об'єднання розподілених інформаційних систем з різними моделями доступу (RBAC, MAC, DAC) [5-10], як показано на рис. 1. Кооперацію цих систем можна умовно розділити на дві фази:

1. Визначення та представлення локальних даних кожної з систем для передачі на глобальний рівень використовуючи формальне визначення елементів для отримання локальної схеми.
2. Декомпозиція локальної схеми на глобальному рівні і призначення кожному з елементів конкретного агента захисту.

Локальний рівень надає опис локальних даних на глобальний рівень, використовуючи відповідні описові елементи, що містять локальну схему даних та власне локальні дані. На локальному рівні формується множина, яка складається з семантичних описових елементів та їх структур захисту для кожної розподіленої системи.

На наступному рівні описаного процесу об'єднання локальних джерел даних формується уніфікована множина, що складається з семантичних описових елементів та структур захисту. На даному рівні визначаються суб'єкти (активні сутності в системі) та об'єкти (дані в системі). Суб'єкти можуть визначати користувачів та процеси, які мають доступ до даних в системі. Інформація (дані в системі) визначає системні об'єкти, дії на яких можуть бути представлені як найбільш популярні операції(читання, запис, модифікація, видалення). Відповідно, можна виділити три основних набори елементів, які описують правила контролю доступом – суб'єкти, об'єкти та операції над даними.

Рівень інтелектуальних агентів включає в себе агентів, а також їхні об'єднання в доменах захищеності на глобальному рівні. Ці агенти призначені для різних типів задач – агенти управління, агенти захисту, семантичні, комунікаційні та організаційні агенти [7-13].

Основною складовою рівня аутентифікації є інтерфейс користувача для авторизації.

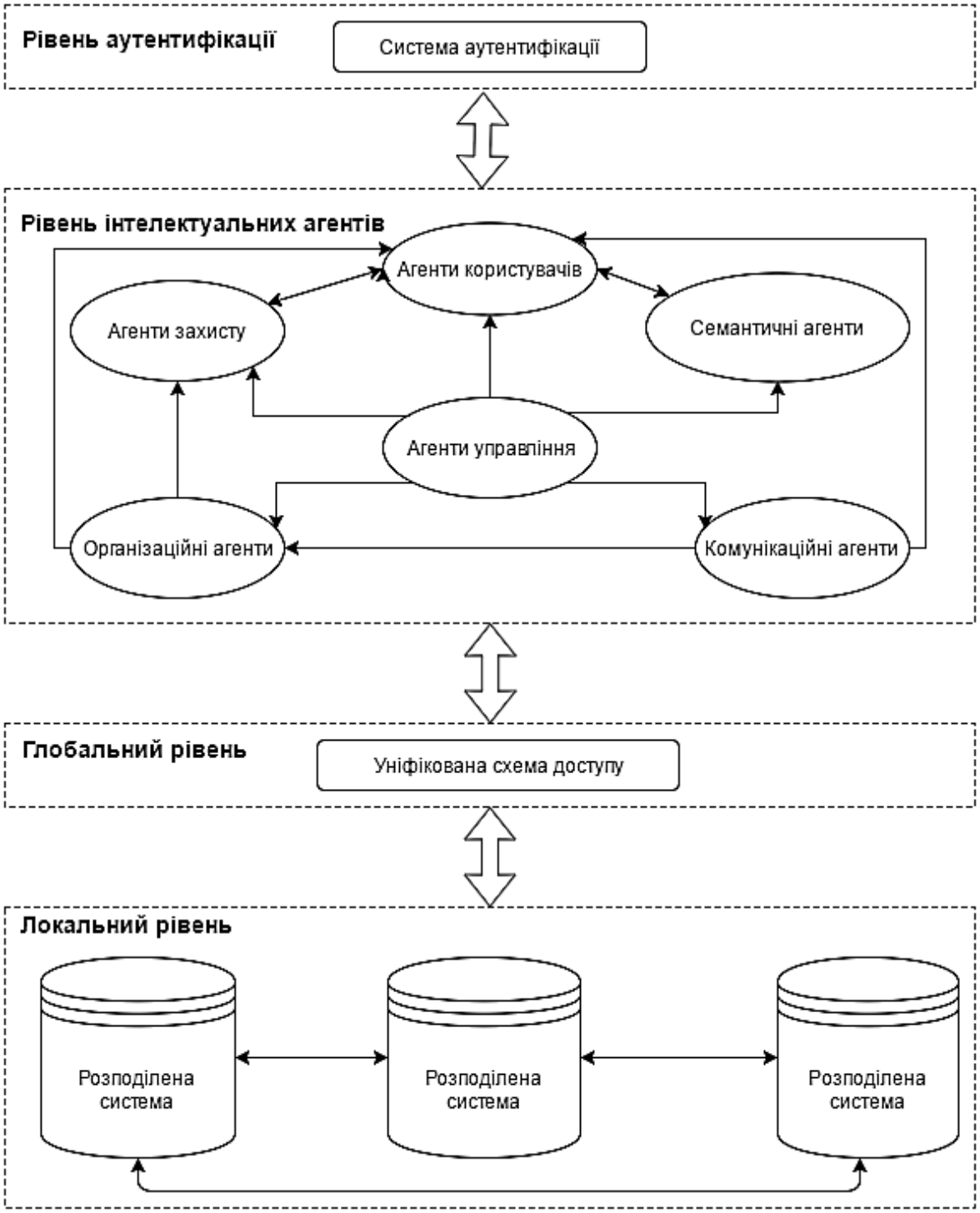


Рис. 1. Структура об'єднання гетерогенних розподілених інформаційних систем з різними рівнями доступу

Підхід з використанням інтелектуальних агентів в контексті захисту об'єднання розподілених систем можна розглядати таким чином, що агенти можуть бути використані:

1. Для підтримки політик безпеки визначених в об'єднання розподілених систем;

2. Для забезпечення захищеності даних чи для вирішення проблем зв'язаних з доступом користувачів в реальному часі.

Для визначення правил в системі для надання користувачам доступу до запитуваних даних чи їх частини.

Розподілені системи також можуть базуватись на комунікації між агентами та комунікації зовнішніх користувачів з агентами. Системи можуть взаємодіяти за допомогою

інтелектуальних агентів, які обмінюються інформацією, займаються пошуком та дослідженням даних в системі. Можливо визначити деякі типи агентів в контексті задачі забезпечення захищеності об'єднання інформаційних систем [9-15]:

- Агенти пошуку – займаються пошуком необхідної інформації в середовищі одних агентів для потреб інших.
- Агенти-дослідники – аналізують інформаційне середовище кожного з агентів для побудови структури даних мультиагентного середовища;
- Агенти обміну даними – несуть відповідальність за обмін інформацією між агентами в мультиагентному середовищі;
- Комунікаційні агенти – керують комунікацією на рівні локальних систем;
- Агенти захисту – керують доменами глобальної захищеності.
- Організаційні агенти – керують відношеннями між елементами між агентами в мультиагентному середовищі.

**2. Модель інтелектуального агента захисту**

Структура інтелектуального агента захисту показана на рис. 2. В його склад входить кілька модулів, які здійснюють обмін даними між собою. На початкових етапах роботи агента, його склад входить достатній набір даних, який дає змогу йому функціонувати та приймати рішення.

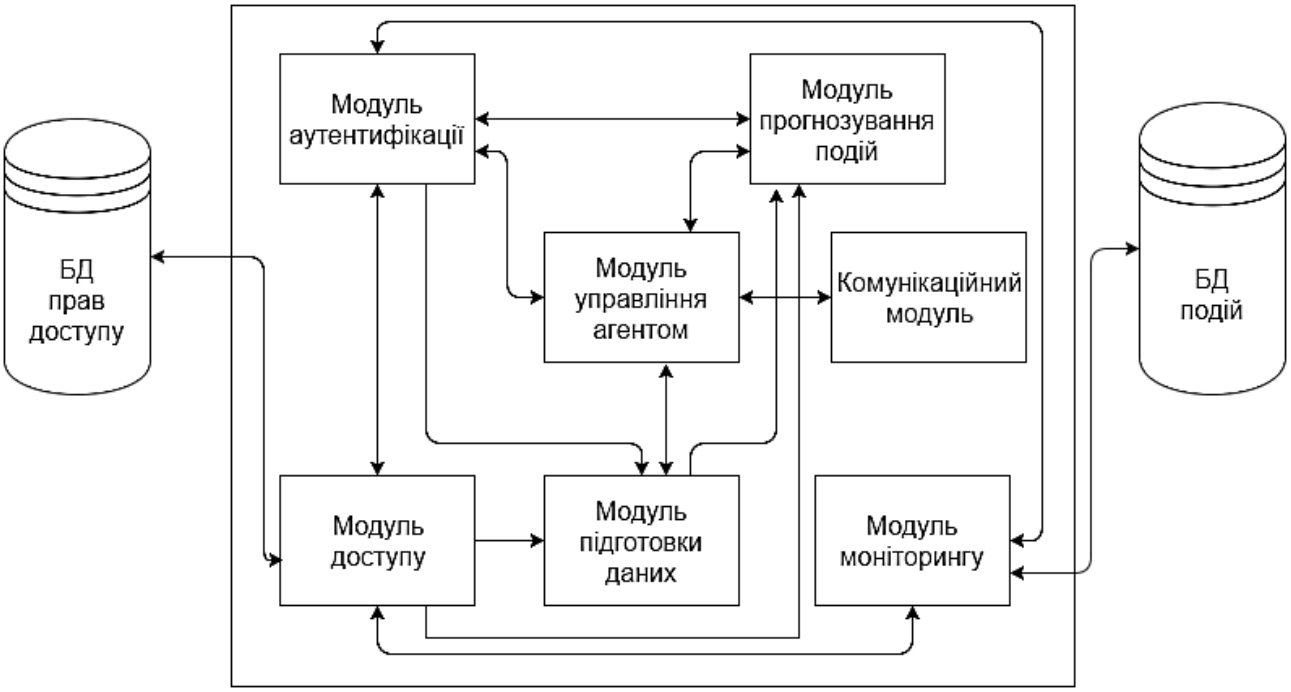


Рис. 2. Структурна модель інтелектуального агента захисту

Розглянемо склад інтелектуального агента захисту детальніше:

*Модуль аутентифікації* обробляє інформацію отриману з системи аутентифікації, перевіряє наявність користувача в системі та коректність отриманих даних при авторизації. У випадку коректної аутентифікації передає повідомлення модулю доступу. Також модуль здійснює комунікацію з модулем розвитку по передачі даних аутентифікації визначеного користувача. Він обмінюється інформацією з модулем прогнозування для передбачення потенційних загроз та модулем моніторингу для збереження інформації про події аутентифікації.

До складу *модуля доступу* входить база даних яка, зберігає права користувачів на виконання операцій в системі та опис набору даних розподіленої системи по відношенню до

яких ці права можуть бути застосовані. Також в даному модулі здійснюється управління наданням прав на роботу з даними в певній розподіленій системі для кожного конкретного користувача.

*Модуль моніторингу* здійснює збір та обробку інформації про роботу користувача в системі. До його складу входить механізм запису інформації про події в розподілених системах, що зв'язані з робою користувача. Дана інформації записується в спеціально виділену БД, в якій визначено кілька видів таблиць для зберігання різних типів даних, що надходять з моніторингу.

До складу *модуля підготовки даних* входить механізм обробки подій в системі, їх фільтрація та передача агенту прогнозування. Наступною функцією даного модуля є розширення бази знань інтелектуального агента за рахунок збереження помилок та спроб несанкціонованого доступу до даних для кожного конкретного користувача.

*Модуль прогнозування подій* відповідає за обробку отриманих даних від модулів аутентифікації, доступу та підготовки для виявлення потенційних загроз та атак в системі. Також здійснює передачу інформації агенту доступу про можливості спроб несанкціонованого доступу до визначеного набору даних.

*Модуль управління* агентом надає інтерфейси зовнішньої взаємодії з даним агентом. Регулює взаємодію модулів в агенті а також зберігає інформацію про стан кожного з них.

*Комунікаційний модуль* регулює взаємодію з агентами в мультиагентному середовищі.

Дана структурна модель інтелектуального агента дозволить забезпечити постійний контроль за діями суб'єктів, які хочуть отримати доступ до даних в гетерогенних розподілених інформаційних системах, а саме:

1. Виконання аутентифікації та авторизації;
2. Операції з даними;
3. Зміна прав інших користувачів.

Структурна модель інтелектуального агента захисту дозволяє взаємодіяти з іншими типами інтелектуальних агентів:

- з агентами пошуку для отримання інформації по даних з інших агентів, яка потрібна для модуля моніторингу;
- з агентами-дослідниками для проведення інформаційного аналізу через модуль прогнозування подій;
- з агентами обміну даними для отримання доступу до даних через модуль доступу;
- з комунікаційними агентами для проведення інформаційного обміну з іншими агентами через комунікаційний модуль;
- з організаційними агентами для обміну інформацією, яка стосується управління через модуль управління агентом.

Ця взаємодія дозволяє підвищити швидкість прийняття рішень інтелектуальним агентом захисту та підвищити ступінь координації між різними агентами, які застосовуються при доступі до розподілених систем.

**3. Перевірка коректності роботи інтелектуального агента**

Для аналізу коректності роботи агента захисту проведено експеримент щодо визначення помилок I та II роду для різної кількості спроб доступу до даних та аутентифікації. Помилкою I роду вважається неправильне трактування загрози як нормальної дії, а помилкою II роду – неправильне трактування звичайної події як загрози.

Експеримент проводився на чотирьох персональних комп'ютерах (процесор 2x2.4 ГГц, ОП 4 Гб, жорсткий диск 500 Гб) на яких встановлено різні операційні системи (Linux, Windows XP, Windows 10). Програма по визначенню помилок I та II роду була написана на Visual studio 2015 C# з використанням бази даних MS SQL.

З результатів експерименту, які зображені на рис. 3 видно, що при збільшенні спроб авторизації та доступу до даних помилки I та II роду зменшуються.

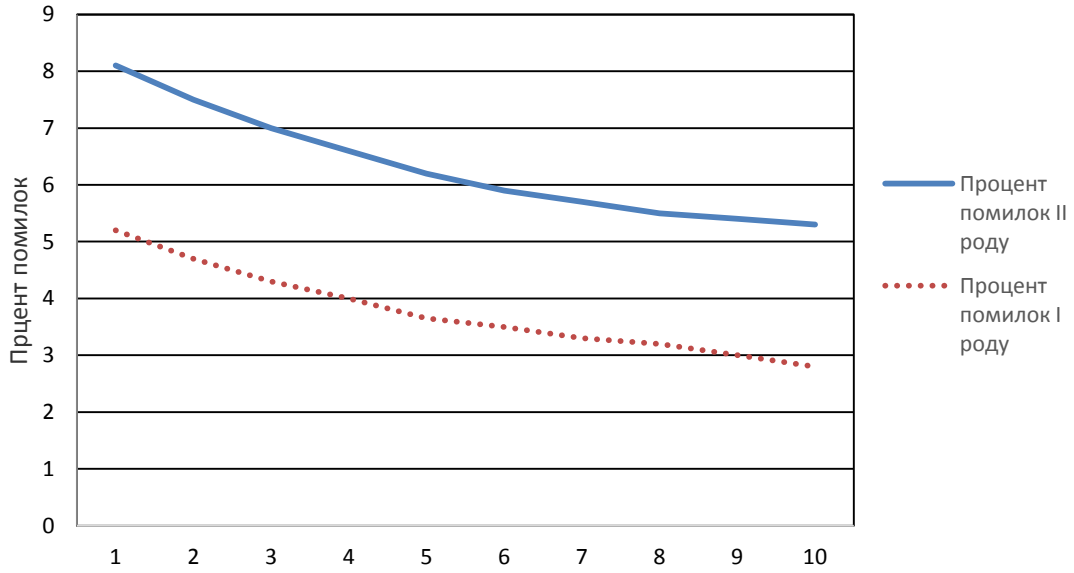


Рис. 3. Обробка подій роботи з даними та авторизації

**Висновок**

В даній статті проведено аналіз основних типів існуючих розподілених систем, визначено загальні особливості та надано загальну класифікацію за різними критеріями. Запропоновано структуру об'єднання розподілених систем з різними моделями доступу. Визначено можливості використання інтелектуальних агентів в розподілених системах. Розглянуто основні типи інтелектуальних агентів та способи їх взаємодії в контексті об'єднання систем з різними моделями доступу. Запропоновано структурну модель інтелектуального агента захисту, його основні модулі та взаємозв'язки між ними. Проведено експериментальні дослідження, які довели, що при збільшені спроб авторизації та доступу до даних зменшується процент помилок I та II роду.

**Література**

1. Kasabov N. Introduction: Hybrid intelligent adaptive systems / N. Kasabov // International Journal of Intelligent Systems. – Vol. 6, 2008. – PP. 453 - 454.

2. Poniszewska-Maranda A. Conception Approach of Access Control in Heterogeneous Information Systems using UML / A. Poniszewska-Maranda // Journal of Telecommunication Systems. – Vol. 45, 2010. – PP. 453 - 454.

3. Oliveira R. Network Management with Knowledge of Requirements: Use of Software Agents / R. Oliveira // PhD Thesis.

4. Corley S. The Application of Intelligent Agent Technologies to Network and Service Management / S. Corley // Proc. of 15th IS&NConference. – Belguim, 2008.

5. Poniszewska-Maranda A., Goncalves G., Hemery F. Representation of extended RBAC model using UML language LNCS / A. Poniszewska-Maranda, G. Goncalves, F. Hemery // Proceedings of SOFSEM 2005: Theory and Practice of Computer Science. – 2005.

6. Lampson B. Authentication in Distributed Systems: Theory and Practice / B. Lampson, M. Abadi, M. Burrows, E. Wobber // ACM. – 2011.

7. Wooldridge M. An Introduction to MultiAgent Systems / M. Wooldridge. – John Wiley & Sons, 2002.

8. Singh M. Readings in Agents / M. Singh, M. Huhns. - Morgan Kaufmann, 2007.

9. Мухин В.Е. Многоуровневая модель с дифференциальным уровнем доверия к субъектам для повышения защищенности распределенных баз данных / В.Е. Мухин, Я.И. Корнага // Научно-технические ведомости Санкт-Петербургского государственного

политехнического университета «Информатика. Телекоммуникации. Управление», №6, 2012. – С. 54 – 58.

10. Muller J.P. The Design of Intelligent Agents – A Layered Approach / J.P. Muller // LNAI state-of-the-art Survey. – 2007. – P. 196.

11. Маслобоев А.В. Мультиагентная система интеграции распределенных информационных ресурсов инноваций / А.В. Маслобоев, М.Г. Шишаев // Программные продукты и системы. – № 4(92), 2007. – С. 30–32.

12. Мухин В.Е. Разработка и реализация политики безопасности в распределенных компьютерных системах / В.Е. Мухин, А.Н. Волокита // Управляющие системы и машины. – № 3, 2010. – С. 78 – 85.

13. Temnyk K.V. Intellectual multiagent personnel control system in the remote employment conditions / K.V. Temnyk // Artificial intelligence. – №1(59), 2013. - P. 14-21.

14. Leonenkov A.V. Fuzzy modeling in the MATLAB and fuzzy TECH environment / A.V. Leonenkov. – SPb.: BVH-Peterburg, 2005. – P. 736.

15. Rutkovskaya D. Neural nets, genetic algorithms and fuzzy systems / D. Rutkovskaya, M. Pylynsky, L. Rutkovsky. – M.: Goryachaya liniya, 2006. – P. 452.

***Автори статті***

**Мухін Вадим Євгенійович –** доктор технічних наук, доцент, професор кафедри обчислювальної техніки, Національний технічний університет України «Київський політехнічний інститут», Київ, Україна. Тел. +38 067 508 76 84. E-mail: v.mukhin@kpi.ua

**Ткач Михайло Мартинович** – кандидат технічних наук, в.о. завідувача кафедри технічної кібернетики, Національний технічний університет України «Київський політехнічний інститут», Київ, Україна.

**Корнага Ярослав Ігорович** – кандидат технічних наук, доцент кафедри технічної кібернетики, Національний технічний університет України «Київський політехнічний інститут», Київ, Україна. Тел. +38 099 224 65 15. E-mail: slovyan_k@ukr.net.

**Мостовий Євгеній Олександрович** – аспірант кафедри технічної кібернетики, Національний технічний університет України «Київський політехнічний інститут», Київ, Україна. Тел. +38 093 672 95 47. E-mail: eugeniy.mostovoy@gmail.com.

**Герасименко Оксана Юріївна** – аспірант кафедри інформаційних та комп'ютерних систем, Чернігівський національний технічний університет, Чернігів, Україна. Тел. +38 099 785 87 58. E-mail: oksgerasymenko@gmail.com.

***Authors of the article***

**Mukhin Vadym Yevgenievich –** doctor of Science (technic), professor of computer engineering department, National Technical University of Ukraine "Kiev Polytechnic Institute", Kiev, Ukraine. Tel. +380 67 508 76 84. E-mail: v.mukhin@kpi.ua

**Tkach Mykhailo Martynovich** – candidate of Science (technic), deputy chair of technical cybernetics department, National Technical University of Ukraine "Kiev Polytechnic Institute", Kiev, Ukraine

**Kornaga Yaroslav Igorovich** – candidate of Science (technic), associate professor of technical cybernetics department, National Technical University of Ukraine "Kiev Polytechnic Institute", Kiev, Ukraine. Tel. +380 99 224 65 15. E-mail: slovyan_k@ukr.net

**Mostovoy Yevgeniy Alexandrovich** – post-graduate student of the technical cybernetics department, National Technical University of Ukraine "Kiev Polytechnic Institute", Kiev, Ukraine. Tel. +38 093 672 95 47. E-mail: eugeniy.mostovoy@gmail.com

**Gerasimenko Oksana Yurievna** – post-graduate student of information and computer systems department, Chervinog National Technical University, Chernigov, Ukraine. Tel. +38 099 785 87 58. E-mail: oksgerasymenko@gmail.com

Дата надходження в редакцію: 18.01.2016 р. Рецензент: д.т.н., проф. Ю.Г. Савченко