Ministry of Education and Science of Ukraine

Odessa National Academy of Food Technologies

International Competition of Student Scientific Works

BLACK SEA SCIENCE 2020

Information Technology, Automation and Robotics

Proceedings

Odessa, ONAFT 2020

UDC 004.01/08

Editorial board:

Prof. B. Iegorov, D.Sc., Rector of the Odessa National Academy of Food Technologies, Editor-in-chief
Prof. M. Mardar, D.Sc., Vice-Rector for Scientific and Pedagogical Work and International Relations, Editor-in-chief
Dr. S. Kotlyk, Ph.D., Assoc. Prof., Director of the P.M. Platonov Educational-Scientific Institute of Computer Systems and Technologies "Industry 4.0", Editor-in-chief
O. Sokolova – Senior Lecturer of the Department of Advanced and Applied Mathematics, ONAFT, Technical Editor

Black Sea Science 2020: Proceedings of the International Competition of Student Scientific Works. Information Technology, Automation and Robotics. / Odessa National Academy of Food Technologies; B.Yegorov, M. Mardar, S.Kotlyk (editors-in-chief.) [*et al.*]. – Odessa: ONAFT, 2020. – 365 p.

These materials of International Competition of Student Scientific Works «Black Sea Science 2020» contain the works of the contest participants in the section «Information technologies, automation and robotics» (not winners).

The author of the work is responsible for the accuracy of the information.

Odessa National Academy of Food Technologies, 2020.

Organizing committee:

Prof. Bogdan Iegorov, D.Sc., Rector of Odessa National Academy of Food Technologies, Head of the Committee

Prof. Maryna Mardar, D.Sc., Vice-Rector for Scientific and Pedagogical Work and International Relations of Odessa National Academy of Food Technologies, Deputy Head of the Committee

Prof. Stefan Dragoev, D.Sc., Vice-Rector for Scientific Work and Business Partnerships of University of Food Technologies (Bulgaria)

Prof. Baurzhan Nurakhmetov, D.Sc., First Vice-Rector of Almaty Technological University (Kazakhstan)

Prof. Mircea Bernic, Dr. habil., Vice-Rector for Scientific Work of Technical University of Moldova (Moldova)

Prof. Jacek Wrobel, Dr. habil., Rector of West Pomeranian University of Technology (Poland)

Prof. Michael Zinigrad, D.Sc., Rector of Ariel University (Israel)

Dr. Mei Lehe, Ph.D., Vice-President of Ningbo Institute of Technology, Zhejiang University (China)

Prof. Plamen Kangalov, Ph.D., Vice-Rector for Academic Affairs of "Angel Kanchev" University of Ruse (Bulgaria)

Dr. Alexander Sychev, Ph.D., Assoc. Professor of Sukhoi State Technical University of Gomel (Belarus)

Dr. Hanna Lilishentseva, Ph.D., Assoc. Professor, Head of the Department of Merchandise of Foodstuff of Belarus State Economic University (Belarus)

Prof. Heinz Leuenberger, Ph.D., Professor of the Institute of Ecopreneurship of University of Applied Sciences and Arts (Switzerland)

Prof. Edward Pospiech, Dr. habil., Professor of the Institute of Meat Technology of Poznan University of Life Sciences (Poland)

Prof. Lali Elanidze, Ph.D., Professor of the Faculty of Agrarian Sciences of Iakob Gogebashvili Telavi State University (Georgia)

Dr. V. Kozhevnikova, Ph.D., Senior Lecturer of the Department of Hotel and Catering Business of Odessa National Academy of Food Technologies, Secretary of the Committee

The jury for the section «Information technologies, automation and robotics»

Head of the jury:

Serhiy Kotlyk – Ph.D., Associate Professor, Director of the P.M. Platonov Educational-Scientific Institute of Computer Systems and Technologies "Industry 4.0" of Odessa National Academy of Food Technologies

Members of the jury:

Francisco Augusto – Dr., International Relations Manager of Higher Institute of Information and Communication Technologies (Angola)

Andrey Kuprijanov – Ph.D., Associate Professor of the Department of Software for Computers and Automated Systems of Belarusian National Technical University (Belarus)

Simon Milbert – Vice-President of Xtra Information Management, Inc. (USA)

Ivan Palov – D.Sc., Professor of University of Ruse "Angel Kanchev" (Bulgaria)

Gerard H. Degla – Communications and Training Manager of "MAPCOM solutions informatiques" company group (Benin)

Viktor Khobin – D.Sc., Professor, Head of the Department of Technological Processes Automation and Robotic Systems of Odessa National Academy of Food Technologies

Valerii Levinskyi – Ph.D., Associate Professor of the Department of Technological Processes Automation and Robotic Systems of Odessa National Academy of Food Technologies

Viktor Yehorov – Ph.D., Supervisor of the Laboratory of Mechatronics and Robotics of Odessa National Academy of Food Technologies

Valeriy Plotnikov – D.Sc., Professor, Head of the Department of Information Technology and Cybersecurity of Odessa National Academy of Food Technologies

Pavlo Lomovtsev – Ph.D., Associate Professor of the Department of Information Technology and Cybersecurity of Odessa National Academy of Food Technologies

Yurii Kornienko – Ph.D., Associate Professor of the Department of Information Technology and Cybersecurity of Odessa National Academy of Food Technologies

Sergii Artemenko – D.Sc., Professor, Head of the Department of Computer Engineering of Odessa National Academy of Food Technologies

Serhii Shestopalov – Ph.D., Associate Professor of the Department of Computer Engineering of Odessa National Academy of Food Technologies

Secretary of the jury:

Oksana Sokolova – Senior Lecturer of the Department of Advanced and Applied Mathematics of Odessa National Academy of Food Technologies

Coopers LLP, NewYork, NY, USA Universit´edu Qu´ebecen Outaouais, Gatineau, Qu´ebec, Canada.

6. Chunarova, A. V., Parhomenko, I. I. & Sashhuk, I. I., (2014). Analysis of approaches and software solutions for the assessment and control of information risks in the computerized. Bulletin of the Engineering Academy of Ukraine, 2:138-142.

7. Buchyk, S. S., (2017). Methodology for assessing information risks in an automated system. Knowledge-based technologies, 3 (35):224.

8. Buchyk, S. S. & Shalaev, V. A., (2017). Analysis of instrumental methods for determining information security risk information and telecommunication systems. Knowledge-based technologies, 3(35):215-225.

9. Puzyrenko, O. G., Ivko, S. O., Lavrut, O. O. & Klymovych, O. K., (2015). Application of information security risk assessment models in information and telecommunication systems. Systems of information processing, 3(128):75-79.

10. Gonchar, S., (2014). Analysis of probability of realization of threats of information protection in automated control systems of technological process. Information protection, 16(1):40-46.

11. C. P. Pfleeger and S. L. Pfleeger, Security in Computing, 4th ed. Englewood Cliffs, NJ: Prentice-Hall, 2006.

12. Sarvin, A., Abakulina, L., (2003). Diagnostics and over automation of systems: Written lectures. SPB.: SZTU. – 69 c.

13. D. Hwang, P. Schaumont, K. Tiri, and I. Verbauwhede, "Securing embedded systems," IEEE Security Privacy, vol. 4, no. 2, pp. 40–49, Mar. 2006.

14. Slobodenuk, D., (2013). Banking technologies, information security tools in banking systems. // http://www.arinteg.ru/about/publications/press/sredstva-zashchity-informatsii-v-bankovskikh-sistemakh-131107.html, 15.01.2020.

15. SS 34.311-95. Information technology. Cryptographic information security. Hash function– K.: SS of Ukraine, 1998.

INTELLIGENT AGENT OF ACCESS MANAGEMENT AND CONTROL SYSTEM

Author: Denys Vysoven
Supervisor: Artem Kovalchuk
National Technical University of Ukraine
«Kyiv Sikorsky Polytechnic Institute» (Ukraine)

Abstract.*This article is devoted to the research and development of an agent for a distributed system of access management and control. It consists of different modules, which allows for addition of new features and improves its security and redundancy capabilities. This system allows for a precise control of movement of authorized and unauthorized personnel.*

Keywords: *distributed systems, multiagent systems, ACS systems, security*

Introduction

In the conditions of fierce competition in the market of new technologies, observance of conditions of secrecy and counteraction of technological information leakage, information security, unauthorized access to equipment and territory for some enterprises, the question of organization and control of access to technological zones and premises becomes critical.

This paper addresses the problem of adapting the access control and management system as a way of managing an object in the context of the changing state of the environment and the object itself (technological zone, etc.).

Adaptation of the access control and management system is based on changing the scenarios of its behavior according to external factors, such as time of day, the presence in the technical area of authorized personnel with higher priority, the presence of authorization in general, etc. In the case of a distributed access control and management system, the possible scenarios for its behavior are much more complicated.

Modern access control and management systems do not have adaptive algorithms for organizing regulations of their operation.

This paper describes the creation of an agent for a distributed system of access control and management to technological zones and premises (hereinafter ACS). Its role is to ensure regulations and scenarios for authorized and unauthorized access and movement of persons within the control area.

In order to ensure a high level of protection of the object against unauthorized interference in a changing situation, the following should be considered:

1. Possibility to change access regulations during the day.
2. Possibility to change access regulations in case of emergencies (fire, accident, terrorist attack, natural disaster, etc.).
3. Possibility to change the regulations for access to the equipment, its activation and / or change of the operating mode according to the access level.
4. Ability to monitor the movements of persons (and their legitimacy) in the control area.

Access control systems

The existing literature about modern access management and control systems describes the following principles of ACS operation [4, 7]:

- countering industrial espionage;
- anti-theft action;
- against sabotage;
- against intentional damage to material assets;
- time tracking;
- controlling the arrival and departure of employees on time;
- protection of confidentiality of information;
- regulation of the flow of visitors;
- control of entry and exit of transport and freight.

In addition, ACS is a barrier to the "curious" people [4].

When implementing specific access control systems, different methods and devices are used to identify and verify a person.

As the most commonly used ACS can be called such [4]:

- regular carousels and walls;
- turnstiles for passage in the corridors;
- lock cabins;
- automatic gates;
- rotating turnstiles;
- revolving doors;
- roadblocks;
- barriers;
- parking systems;
- sliding round doors;
- three-bar turnstiles;
- full-height turnstiles;
- sliding turnstiles.

A very important issue is the possibility of integrating ACS with any security system using an open protocol [4].

The main objectives of the checkpoint regulations are [4, 7]:

- protecting the legitimate interests of the plant, maintaining internal management;
- protection of business property, its rational and efficient use;
- increase in corporate profits;
- internal and external stability of the organization;
- protection of trade secrets and intellectual property rights.

Checkpoint regulations as part of the security system allows owner to solve the following tasks [4, 7]:

- Ensuring licensed transition of employees and visitors, import / export of material products and assets, butchering of enterprise;
- Preventing uncontrolled penetration of unauthorized persons and vehicles into protected areas and private buildings (premises);
- Timely identification of threats to the interests of the plant, as well as potentially dangerous conditions that could cause material and moral harm to the venture;
- Creating reliable guarantees for maintaining the organizational stability of the external and internal relationships of the enterprise, developing a rapid response mechanism for threats and negative trends;
- Suppression of outbreaks in the legitimate interests of the enterprise, the use of legal, economic, organizational, socio-psychological, technical and other means to identify and reduce sources of threat to the security of the enterprise.

Checkpoint regulations can be defined as a system of providing regulatory, organizational and material guarantees for identifying, preventing and combating infringement of the legal rights of an enterprise, its property, intellectual property, production discipline, technological leadership, scientific achievements and protected information, and as a combination of organizational and legal restrictions and rules, establishing the procedure for passing through the checkpoint employees of the facility, visitors, transport of import / export of material assets [4].

Multi agent systems

An agent is a computer system located in a particular environment, and can operate autonomously in that environment to meet its design goals.

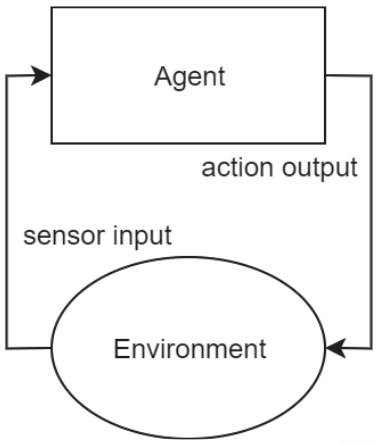

Figure 1. An agent in its environment. The agent takes sensory input from the environment, and produces as output actions that affect it. The interaction is usually an ongoing, non-terminating one.

Figure 1 gives an abstract view of an agent. In this diagram, we can see the action output generated by the agent in order to affect its environment. In most areas of reasonable complexity, an agent will not have complete control over its environment. It will have at best partial control, in that it can influence it. From the agent's point of view, this means that the same action performed twice in apparently identical circumstances might appear to have completely different effects, and in particular, it may not have the desired effect. Therefore, agents should be prepared in environments other than the most natural for the possibility of failure. We can formally summarize the situation by saying that environments are in general assumed to be nondeterministic. Usually, an agent will have a variety of actions available to it. This set of possible actions represents its ability to change its environment. Note that not all actions can be performed in all situations. For example, an action 'lift table' is only applicable in situations where the weight of the table is sufficiently small that the agent can lift it. Similarly, the action 'purchase a Ferrari' will fail if insufficient money are available to do so.Operations therefore have preconditions that define the possible situations in which they can be applied. The key problem facing an agent is that of deciding which of its actions it should perform in order to best satisfy its design objectives. Agent architectures are really software architectures for decision-making systems that are embedded in an environment [1, 2, 5, 6].

Control system can be viewed as an agent. A simple example of such a system is a thermostat. Thermostats have a sensor for detecting room temperature. This sensor is embedded directly in the environment (i.e. the room), and it produces as output one of two signals: one that indicates that the temperature is too low, another, which indicates that the temperature is OK. The actions available to the thermostat are 'heating on' or 'heating off'. The action 'heating on' will generally have the effect of raising the room temperature, but this cannot be a guaranteed effect - if the door to the room is open, for example, switching on the heater may have no effect. The (very simple) decision making component of the

thermostat implements (usually in electro-mechanical hardware) the following rules [1, 3, 6]:

- too cold - heating on,
- temperature OK - heating off.

More complex environment control systems, of course, have considerably richer decision structures. Examples include autonomous space probes, fly-by-wire aircraft, nuclear reactor control systems, and so on [1, 5].

Main conditions of agents' intelligence [1]:

- Reactivity. Intelligent agents are able to perceive their environment, and respond in a timely fashion to changes that occur in it in order to satisfy their design objectives.
- Proactiveness. Intelligent agents are able to exhibit goal-directed behaviour by taking the initiative in order to satisfy their design objectives.
- Social ability. Intelligent agents are capable of interacting with other agents (and possibly humans) in order to satisfy their design objectives.

Research result

Within the performed work, the concept and the software-hardware complex of the distributed access control and management system were developed.

The developed system consists of three basic parts:

- ACS management Interface;
- Lock Agent;
- Agent for activity monitoring and decision-making.

The software system of the information system has the structure shown in Figure 2.

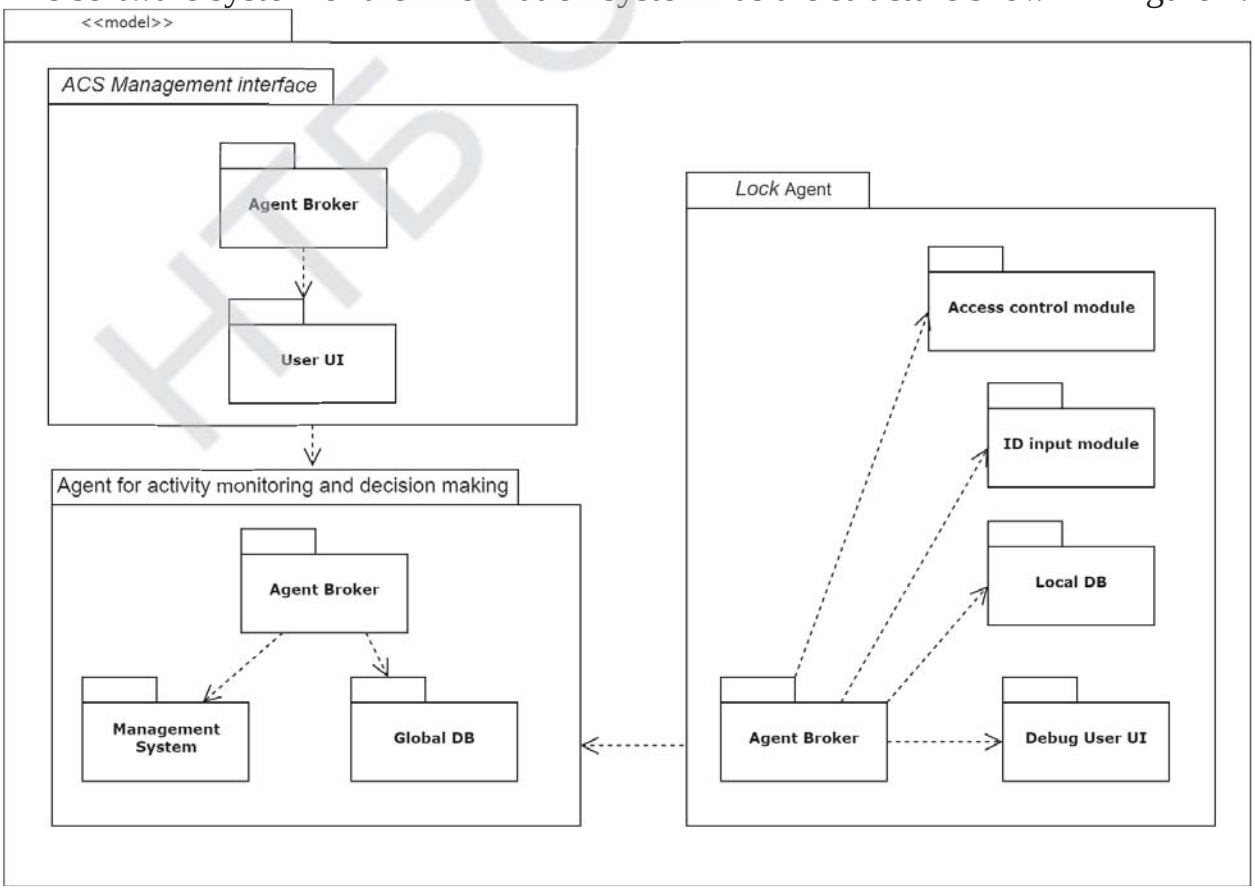

Fig. 2 Structure of the information system

The ACS management interface and the activity monitoring and decision-making agent are software implementations. The lock agent is a hardware and software complex.

The hardware implementation of a lock agent is based on an ARM32-compliant microcomputer, reader modules and access modules (lock actuator, turnstile, power supply, etc.).

The lock agent software is developed in Java programming language, using Hibernate, Netty and GSON libraries and runs on Java Runtime Environment 8 under Armbian Linux operating system.

The admin interface software is designed using the Java programming language, including the Vaadin Framework, using Netty and GSON libraries, and runs on Java Runtime Environment 8.

The activity monitoring and decision-making agent software is developed in Java programming language, including Spring framework, using Netty library and runs on Java Runtime Environment 8.

Each lock agent has a built-in local H2 database in which it stores access rules. The activity monitoring and decision-making agent operates a global database (it is unique to one defined distributed system) MySQL. The management interface manages a copy of the global database. Any changes to the rules coming from the management interface are made to the global database. The activity monitoring and decision-making agent, upon receipt of the new regulation, shall make appropriate adjustments to the system. All changes to the regulation are synchronized with the lock agents, according to the following parameters:

- each lock agent receives only those parts of the regulation that relate to his control area;
- each lock agent receives a minimum amount of personal information.
- data exchange is performed by standardized JSON serialization commands

The software part performs the following main tasks:

- Activation of the system and updating of local databases of lock agents.
- Formation of access regulations by the system administrator according to different situations (fire, accident, terrorist attack, natural disaster, etc.).
- Monitoring of the technical state (status) and controllability of lock agents by the monitoring and decision-making agent.
- Reading information using the readout module.
- Identification of the person by the lock agent using build-in database and determination of permissions of authorized and unauthorized persons.
- Logging events to the system log.
- Monitoring the activity and displacement of individuals.
- Generation of notifications and alarms.
- Prepare and report on relevant services (managers, security and safety services).

The ACS management interface is shown in Figure 3, 4 and 5. It provides the system administrator with the following tools:

- Allows access to the operator's personal cabinet (personal data, identification keys, access keys, etc.).
- Formulation of a list of situations and regulations of access and activity of authorized and unauthorized persons and scenarios of reactions to all possible events.

- Maintenance of a global database of authorized persons.
- Visualization of activities and movements within the control area.
- Monitoring of the status of technical equipment of the ACS.
- Generate reports for different services.

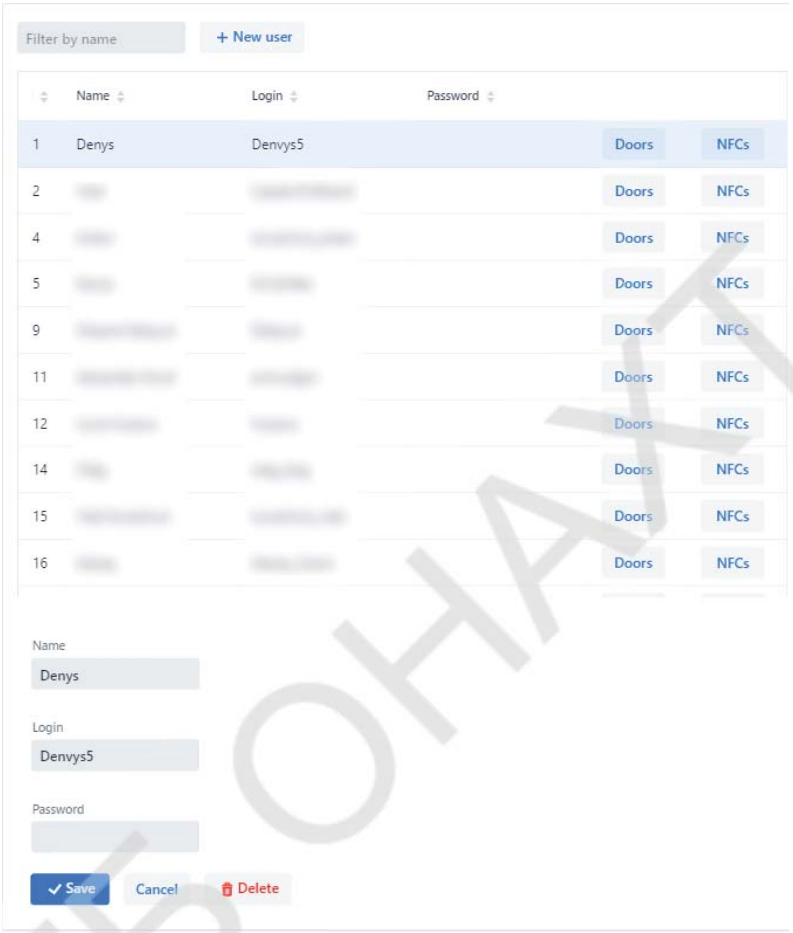

Fig. 3 User List Interface

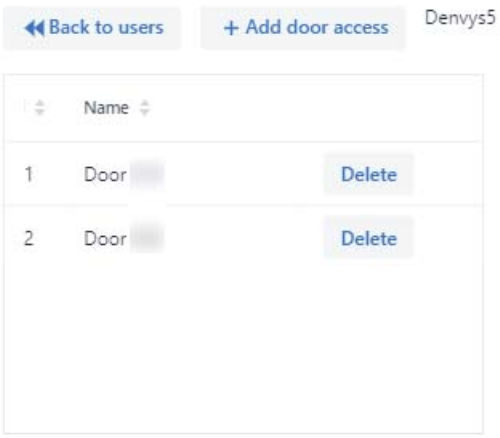

Fig. 4 List of user-accessible premises interface

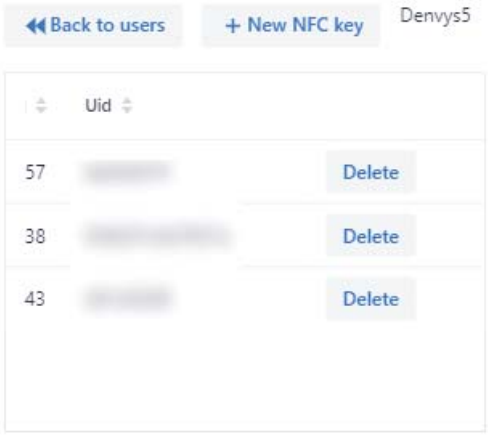

Fig. 5 User authentication keys interface

The lock agent constantly communicates with the monitoring and decision-making agent. Its main task is to enforce the access regulations to the premises on which it is assigned. The lock agent provides the possibility of authorization of persons according to the following identification data:

- credit card
- fingerprint
- personal smartcard
- face scan
- etc.

Conclusion

The result of conducted research is the creation of a multi-agent distributed ACS. It allows you to set rules for access of authorized and unauthorized persons to premises or territories controlled by the system.

This agent allows the multi-agent system to track the movement of people through controlled premises and respond accordingly to the movement of authorized personnel.

This development has the greatest potential in facilities with a high level of security and a large hierarchy of access to premises or territories. After consultations, the military service and large business companies became interested in this development.

The introduction of such a control system will allow enterprises with a high level of internal security to increase the savings of internal resources (by controlling the number of people in different zones and premises of buildings), to improve the details of reporting (about the movement of authorized personnel inside objects controlled by the system) and to reduce the volume of overhead maintenance costs for access control and control systems.

References

1. Wooldridge M.J. An introduction to multi-agent systems. Wiley, 1996
2. Тарасов В.Б. От многоагентных систем к интеллектуальным организациям. Философия, психология, информатика. М., Эдиториал. 2002
3. Ghallab M., Nau D., Traverso P. Automated planning: Theory & Practice. Morgan Kaufmann, 2004
4. Ворона В. А., Тихонов В. А. В83 Системы контроля и управления доступом. - М.: Горячая линия Телеком, 2010

5. Bellifemine F, Caire G, Greenwood D (2007) Developing multi-agent systems with JADE. Wiley, London

6. D. Dimarogonas, E. Frazzoli, K. Johansson, "Distributed event-triggered control for multi-agent systems", IEEE Trans. Autom. Control, vol. 57, no. 5, 2012.

7. Benantar, Messaoud. (2006). Access control systems. Security, identity management and trust models. Access Control Systems: Security, Identity Management and Trust Models. 10.1007/0-387-27716-1.

EMPLOYEES NOTIFICATION SYSTEMS IN THE EVENT OF EMERGENCY SITUATIONS THROUGH PUBLIC WIRELESS ACCESS POINTS

Authors: Oleksiï Patlaichuk, Hlib Serbulov
Supervisors: Sergii Bozhatkin, Victoryia Guseva-Bozhatkina
Admiral Makarov National University of Shipbuilding (Ukraine)

Abstract. *In the event of an emergency, there are still actions that people must take to save themselves. Currently everyone has a mobile phone. Almost all establishments have an open Wi-Fi network. Therefore, the purpose of the work is to design and develop a system that, when connected to the network, informed about the threats that have arisen and the actions that citizens must take to avoid damage. The alert system works around the clock. It complements the existing fire alarm and security systems.*

In the work a critical analysis of existing and prospective emergency alert systems was carried out, which showed that there is currently a revision of the requirements for the civil protection notification system towards the transition to new structures of such systems organization, taking into account the current state of technical means of communication, protection against unauthorized access and the spread of malware, identified the possibility of improving them.

The mathematical model of choosing the optimal coverage of the territory with the signal WI-FI alert has been improved, which takes into account losses during repeated passage of the signal through obstacles, which allows to predict the frequency reuse on different floors of the building.

The study was made on 19 pages of printed text, contains 3 drawings and a list of references, which consist of 22 sources. The study was done in English.

Key words: *Alerts, Public Wireless APs, Unauthorized Data Access, Alert Nodes, Emergencies.*

Introduction

One of the main ways of protecting the population from emergencies is timely notification of the danger in the situation that has arisen as a result of its development, as well as informing about the procedure and rules of behavior in the context of the emergency.

Today there is a revision of the requirements regarding modern alert systems (AS), which were created for the purpose of civil protection tasks by means of automated systems of centralized notification, communication networks, radio broadcasting. There is a transition to new structures of organization of such systems, taking into account the