UDC 004.942

V. S. KHARCHENKO, V. V. SKLYAR

National Aerospace University "KhAI", Ukraine

ASSURANCE CASE DRIVEN DESIGN FOR SOFTWARE AND HARDWARE DESCRIPTION LANGUAGE BASED SYSTEMS

The Claim-Argument-Evidence (CAE) approach is one from the worldly recognized technique directed to find gaps in safety-related Instrumentation and Control systems design and implementation and after that to justify meeting regulatory requirements. An advance approach to improve Assurance (Security and Safety) Case is proposed in a view of Assurance Case Driven Design (AC DD). A practical using of AC DD lays in cost-effectiveness improvement of certification and licensing processes. General framework for AC DC as well as update for CAE in view of Development-Verification & Validation-Assurance Case (DVA) notation are proposed in the paper.

Key words: *Assurance Case, Safety and Security Life Cycle, Claim-Argument-Evidence.*

Introduction

The production of a Safety Case is now required by various standards in safety-critical industries [1]. The Claim-Argument-Evidence (CAE) approach is one from the worldly recognized technique directed to find gaps in safety-related I&C systems design and implementation and after that to justify meeting regulatory requirements [2]. From the point of system features view, the CAE can support Safety Case, Security Case or Assurance Case. The last one usually combines both safety and security features. Case based assessment evolution, in our opinion, is caused by changing of paradigm of system description notation what is presented on Fig. 1.

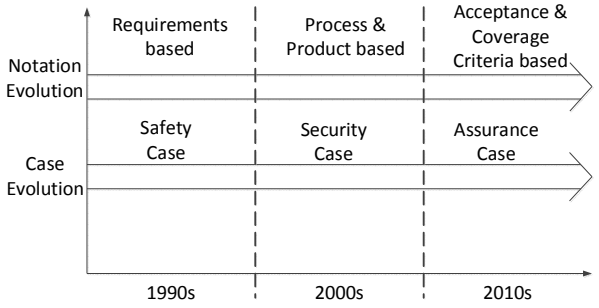

Fig. 1. Case Assessment Evolution for Critical Systems

The third part safety assessment is usually implemented for safety-related Instrumentation and Control (I&C) systems as a part of licensing framework. At the same time a good engineering practice is to implement a desired property, e.g. safety, as soon as possible. For example, Systems Theoretic Accident Model and Process (STAMP) based on systems theory has been developed by Nancy Leveson to explain systems accidents [3]. Safety Driven Design is a part STAMP providing the following general methodology levels:

– top level system and safety engineering;
– after that model generation;
– after that – model-based analysis.

At the same time a goal of security and safety analysis is not only proving a conformance with requirements but mostly discovering gaps in such conformance assessment approach. Assurance (Security and Safety) Case methodology contains a potential for improvement safety and security analysis techniques and tools. We name a set of Assurance Case based techniques and tools as Assurance Case Driven Design (AC DD). A practical using of AC DD lays in improvement of certification and licensing processes.

From this prospective Assurance Case may be implemented for the earliest stages of life cycle activities to drive safety implementation from the scratch.

We name such technique as Assurance Case Driven Design (AC DD). The main motivation of AC DD is the following:

– to develop a technique to assess safety and security features as soon as possible during development of a system concept (specification, design);

– to develop a technique to develop a system concept (specification, design) in a safe and secure manner.

AC DC also supports the following important topics:

– research of integral security and safety features of modern critical control and communication systems and networks as an integral property; security importance increasing requests implementation of security requirements as a part of licensing issues; such approach is named as Security Informed Safety Case [4]; such approach is targeted to analyze safety and security in a structured way and creating Security Informed Safety Case that provide justification of safety taking into particular consideration the impact of security [5, 6];

– research of Field Programmable Gates Arrays (FPGAs) as an alternative to microprocessor units (MCUs) in critical applications;

– research applications for specific market, for example, this paper contains a case study for nuclear safety-critical domain.

This paper target is to provide fundamentals of AC DD for the future improvement and development.

1. General Framework for AC DD

New methodology implementation requires not only technical measures but also organizational efforts to improve involved parts collaboration.

A chart on Fig. 2 demonstrates such collaboration of the following three parts during AC DD implementation:

– design team responsible for a product development;

– Quality Assurance (QA) and/or safety and security management team responsible for following all quality, safety and security procedures during development, verification and validation (V&V), configuration management, audits and other relevant activities;

– assessment and certification team as a third part responsible for independent safety or security assessment of a product usually with issuing of a formal conformance document.

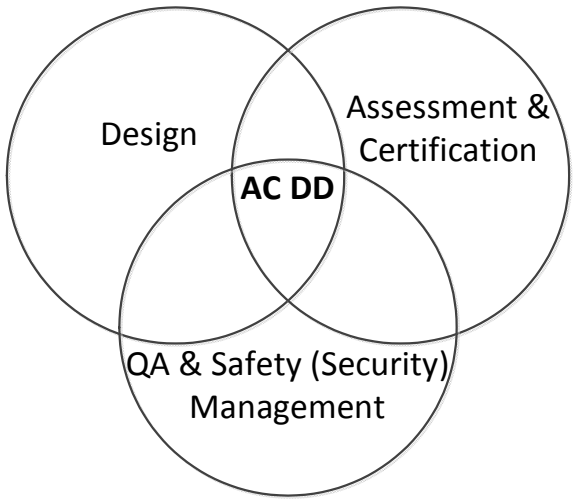

Fig. 2. Assurance Case Driven Design Collaboration Chart

After establishment of organization and collaboration aspects let's analyze a general AC DD framework (see Fig. 3).

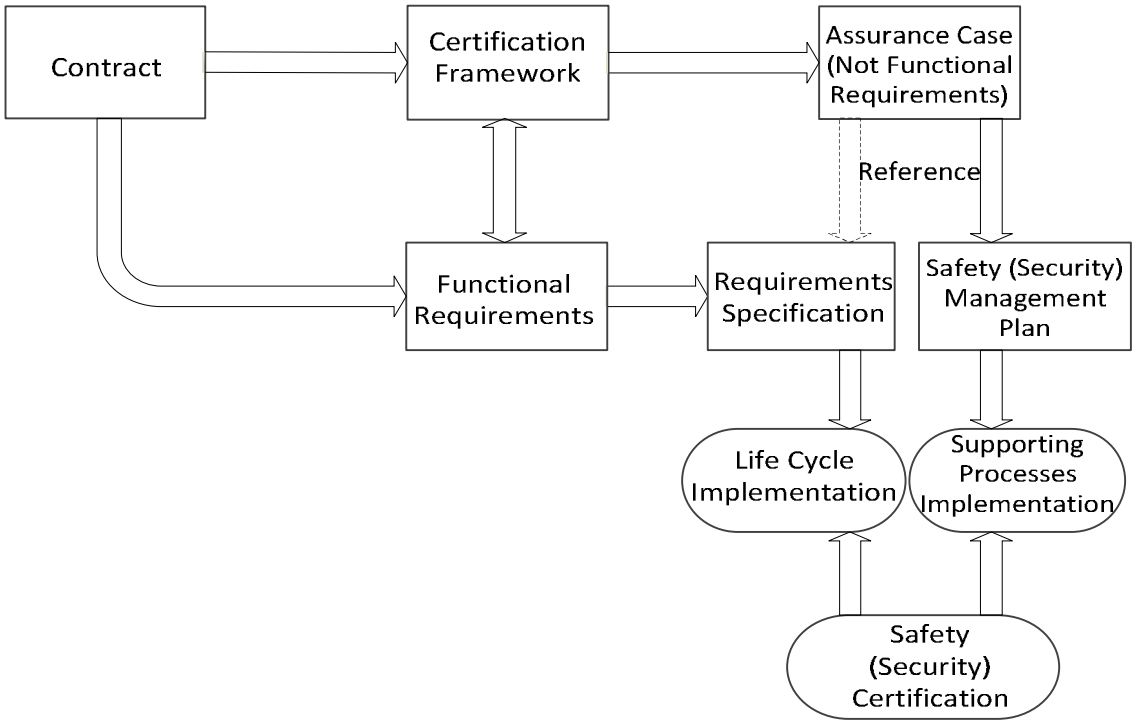

Fig. 3. General Framework for Assurance Case Driven Design

Usually the first step in any system development is signing a contract. This contract is an input for system functional requirement as well as certification or licensing framework for safety and security critical applications. The Requirement Specification has to be developed on the base of contractual functional requirements. Safety and security critical systems shall have an important addition to the Requirement Specification describing not functional requirements targeted to implement system integrity. AC DD approach proposes to present such requirements in a view of a preliminary Assurance Case. Such preliminary Assurance Case is not a result of assessment but a target which has to be achieved after the system implementation. Not functional requirements of Assurance Case are an input for Safety or Security Management Plan which has cover life cycle description with all development support processes. Some parts of not functional requirements (for example, self-diagnostic requirements) may affect the Requirement Specification. After that staged life cycle with V&V and other supporting processes activities (Project Management, Configuration Management and other) has to be implemented in accordance with Safety (Security) Management Plan. After the contract and the Requirement Specification stages life cycle usually includes design, implementation, integration, validation, installation, and commissioning stages. Assurance Case activities have to be implemented after each of the stage. Safety or security certification has to finalize system life cycle before transfer it in operation at the customer site. Also during operation a periodical assessment or certification has to be done with associated update of Assurance Case.

2. CAEC and DVA Notations for AC DD Support

There are two the main notation used for Assurance Case [7]:

– Claim-Argument-Evidence (CAE);

– Goal Structured Notation (GSN).

In the AC DD framework we propose some addition for Assurance Case CAE notations to be able assess specific features of critical systems. Acceptance criteria and coverage criteria are two additional entities which have to be taken into account for support arguments and evidences. Acceptance criteria are the conditions when stated requirements are met. From the point view of Assurance Case, acceptance criteria provide us ability to state the right arguments which are consistent with the claim and to provide the evidences which are consistent with the arguments. Coverage criteria describe how completely the claim is met. From the point view of Assurance Case, coverage criteria provide us ability to state multiple arguments to completely cover all claim features and to provide multiple evidences which completely cover the arguments. A modified CAE notation which we name Claim-Argument-Evidence-Criteria (CAEC) notation is given on Fig. 4.

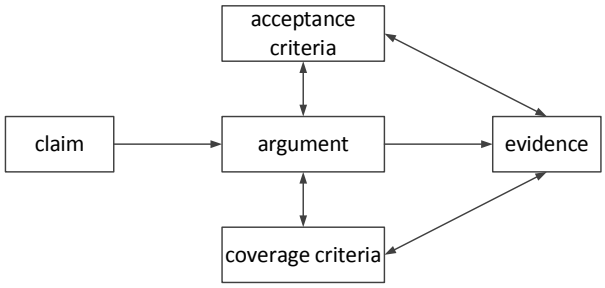

Fig. 4. Claim-Argument-Evidence-Criteria (CAEC) Notation

The next step of CAE / CAEC notation development is to support activities of Safety & Security Life Cycle (SLC) stages with implementation of Assurance Case. Specification and design requirements are the inputs for each of the SLC stage. After any stage fulfillment, requirements implementation assessment has to be performed. This fundamental of the SLC has to be supplemented by the project specific products, processes, tools and techniques (see Fig. 5).

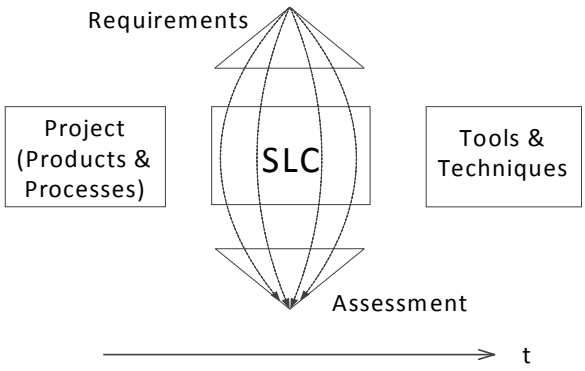

Fig. 5. Requirements based Assessment during Safety & Security Life Cycle

The following activities are mandatory for each of the SLC stage:

– development targeted to move an implemented product representation stage by stage through SLC;

– V&V targeted to check conformance of the SLC stage development outputs to the SLC stage development inputs;

– assurance Case update based on assessment of performed development and V&V activities.

The above can be represented as a diagram given on Fig. 6.

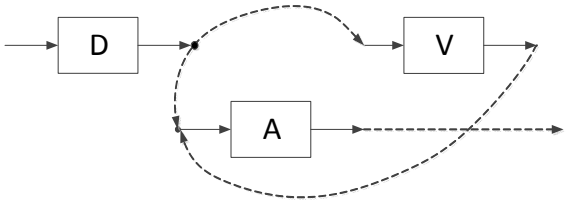

Fig. 6. Development-V&V-Assurance Case (DVA) Notation

3. Implementation of AC DD in Certification and Regulatory Activities

In 2014 the Field Programmable Gates Array (FPGA) based safety platform RadICS [8,9] has been successfully certified against functional safety requirements of the standard IEC 61508 [10]. The company *exida LLC* provided a service for independent certification [11, 12]. Assurance Case for this project shall provide evidence of the RadICS platform compliance with all of 737 requirements of the seven parts of the IEC 61508. Such huge amount of required to perform systematic approach with implementing of top-down development of Assurance Case. As a result of functional safety requirements structured analysis, twenty four parts have been recognized as sections of the general Assurance Case (see Fig. 7).

AC DD for the platform RadICS functional certification included the following activities:

– Preliminary Assurance Case development;

– Combination of safety and security features in one Assurance Case;

– Safety Life Cycle model based on DNA-notation;

– Requirement management and tracing;

– Model-based Design and Testing (MBD and MBT)

– V&V coverage multi-criteria application;

– Resource effective certification strategy implementation;

– Final assessment, Assurance Case release and certification.

Today the RadICS platform has a lot of implementation reference for NPPs around the world. The components of AC DD have been used to achieve functional safety, security, certification, and regulatory licensing goals.

The following projects for nuclear industry around the world based on RadICS platform have been implemented using AC DD:

– 2013-2014, Safety Window Annunciators for Embalse NPP (Argentina) designed in cooperation with Candu Energy (Canada);

– 2014-2015, FPGA-based Test System for joint R&D project with Electricite de France;

– 2015-2016, Control Consol and Nuclear Channels for IEA-R1 Research Reactor of IPEN Research Institute (Brasil);

– Since 2015, licensing of RadICS platform according to requirements of the United States Nuclear Regulatory Commission.

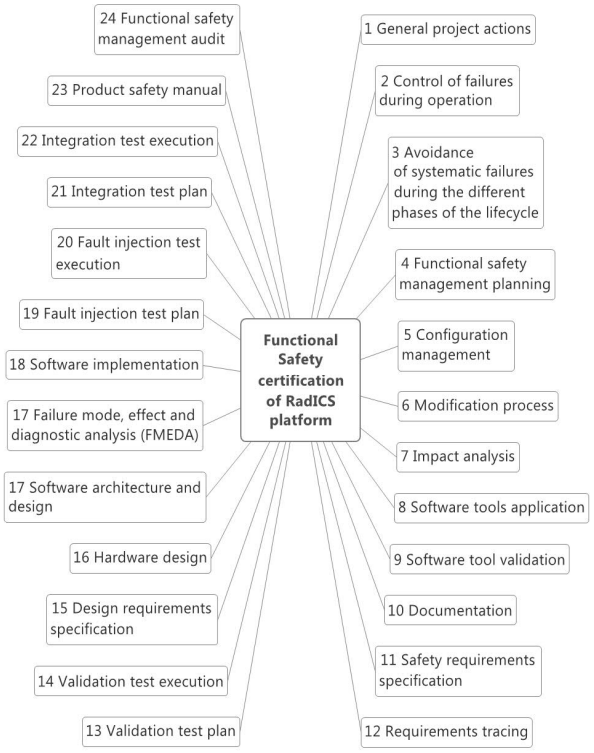

Fig. 7. General Assurance Case diagram for AC DD of FPGA-based safety platform RadICS

Conclusion

The proposed AC DD approach may provide some benefits on the base of from cost-effective as named "embedded certification" briefly described by DVA notation. This cost-effective solution can work under conditions when the total cost of life cycle with application of "embedded certification" would be less then the cost of usual life cycle with usual after life cycle certification, i.e.:

Cost (DVA Life Cycle) < Cost (DV Life Cycle) + Cost (Certification).

The next practical steps of AC DD development have to be directed to analyze existing Safety and

Assurance Cases for the mentioned RadICS platform as well as to enforce Safety Case for FPGA-based nuclear products with Security Informed approach.

References (GOST 7.1:2006)

1. Guerra, S. Understanding, assessing and justifying I&C systems using Claims, Arguments and Evidence [Text] / S. Guerra // Nuclear Safety and Simulation. – 2014. – Vol. 5. – P. 15-26.

2. Toulmin, S. The Uses of Argument [Text] / S. Toulmin. – Cambridge University Press, 1958. – 575 p.

3. Leveson, N. A New Accident Model for Engineering Safer Systems [Text] / N. Leveson // Safety Science. – 2004. – Vol. 42. – P. 237-270.

4. Combination of safety integrity levels (SILs): A study of IEC61508 merging rules [Text] / Y. Langeron, A. Barros, A. Grall, C. Berenguer // Journal of Loss Prevention in the Process Industries. – 2008. – №. 21(4). – P.437-449.

5. Bloomfield, R. Security-Informed Safety: If it's not secure, it's not safe [Text] / R. Bloomfield, K. Netkachova, R. Stroud // Proceedings of 5th International Workshop on Software Engineering for Resilient Systems (SERENE'2013). – Kiev, Ukraine, 2013. – P. 58-67.

6. Security-Informed Safety Case Approach to Analysing MILS Systems [Text] / K. Netkachova, K. Müller, M. Paulitsch, R. Bloomfield // Proceedings of International Workshop on MILS: Architecture and Assurance for Secure Systems. – Amsterdam, the Netherlands, 2015. – P. 12-18.

7. The MILS Component Integration Approach to Secure Information Sharing [Text] / C. Boettcher, R. Delong, J. Rushby, S. Wilmar // Proceedings of 27th Digital Avionics Systems Conference (DASC'2008). – St. Paul, MN, USA, 2008. – P. 154-160.

8. FPGA-based NPP Instrumentation and Control Systems: Development and Safety Assessment [Text] / E. S. Bakhmach, A. D. Herasimenko, V. A. Golovyr, V. S. Kharchenko, Yu. V. Rozen, A. A. Siora, V. V. Sklyar, V. I. Tokarev, S. V. Vinogradskaya, M. A. Yastrebenetsky ; edits V. S. Kharchenko, V. V. Sklyar // Research and Production Corporation "Radiy", National Aerospace University named after N.E. Zhukovsky "KhAI", State Scientific Technical Centre on Nuclear and Radiation Safety, 2008. – 188 p.

9. NUREG/CR-7006 – Review Guidelines for Field-Programmable Gate Arrays in Nuclear Power Plant Safety Systems [Text]. – Oak Ridge National Laboratory, 2010. – 208 p.

10. IEC 61508-1:2010 – Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements [Text]. – European Committee for Electrotechnical Standardization, 2010. – 68 p.

11. Medoff, M. Functional Safety – An IEC 61508 SIL 3 Compatible Development Process [Text] / M. Medoff, R. Faller – exida.com L.L.C., Sellersville, PA, USA, 2010. – 456 p.

12. FPGA-based I&C applications in NPP's modernization projects: Case study [Text] / A. Andrashov, I. Bakhmach, V. Sklyar, A. Kovalenko // Proceeding of the 9th International Conference on Nuclear Plant Instrumentation, Control & Human-Machine Interface Technologies (NPIC&HMIT 2015), Charlotte, NC, USA, 2015. – P. 238-251.

References (BSI)

1. Guerra, S. Understanding, assessing and justifying I&C systems using Claims, Arguments and Evidence. *Nuclear Safety and Simulation*, 2014, vol. 5, pp. 15-26.

2. Toulmin, S. *The Uses of Argument*. Cambridge University Press, 1958. 575 p.

3. Leveson, N. A New Accident Model for Engineering Safer Systems. *Safety Science*, 2004, vol. 42, pp. 237-270.

4. Langeron, Y., Barros, A., Grall, A., Berenguer, C. Combination of safety integrity levels (SILs): A study of IEC61508 merging rules. *Journal of Loss Prevention in the Process Industries*, 2008, no. 21(4), pp.437-449.

5. Bloomfield, R., Netkachova, K., Stroud, R. Security-Informed Safety: If it's not secure, it's not safe. *Proceedings of 5th International Workshop on Software Engineering for Resilient Systems (SERENE'2013)*. Kiev, Ukraine, 2013, pp. 58-67.

6. Netkachova, K., Müller, K., Paulitsch, M., Bloomfield, R. Security-Informed Safety Case Approach to Analysing MILS Systems. *Proceedings of International Workshop on MILS: Architecture and Assurance for Secure Systems.* Amsterdam, the Netherlands, 2015, pp. 12-18.

7. Boettcher, C. Delong, R., Rushby, J., Wilmar, S. The MILS Component Integration Approach to Secure Information Sharing. *Proceedings of 27th Digital Avionics Systems Conference (DASC'2008).* St. Paul, MN, USA, 2008, pp. 154-160.

8. Kharchenko, V. S., Sklyar, V. V. (Edits). *FPGA-based NPP Instrumentation and Control Systems: Development and Safety Assessment*. Research and Production Corporation "Radiy", National Aerospace University named after N. E. Zhukovsky "KhAI", State Scientific Technical Centre on Nuclear and Radiation Safety, 2008. 188 p.

9. *NUREG/CR-7006 – Review Guidelines for Field-Programmable Gate Arrays in Nuclear Power Plant Safety Systems*. Oak Ridge National Laboratory, 2010. 208 p.

10. *IEC 61508-1:2010 – Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*. European Committee for Electrotechnical Standardization, 2010. 68 p.

11. Medoff, M. Faller, R. *Functional Safety – An IEC 61508 SIL 3 Compatible Development Process*. exida.com L.L.C., Sellersville, PA, USA, 2010. 456 p.

12. Andrashov, A., Bakhmach, I., Sklyar, V., Kovalenko A. FPGA-based I&C applications in NPP's modernization projects: Case study. *Proceeding of the 9th International Conference on Nuclear Plant Instrumentation, Control & Human-Machine Interface Technologies (NPIC&HMIT 2015).* Charlotte, NC, USA, 2015, pp. 238-251.

Поступила в редакцию 17.03.2016, рассмотрена на редколлегии 14.04.2016

ПРОЕКТИРОВАНИЕ НА ОСНОВЕ ASSURANCE CASE ДЛЯ СИСТЕМ С ИСПОЛЬЗОВАНИЕМ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ЯЗЫКОВ ОПИСАНИЯ АППАРАТУРЫ

В. С. Харченко, В. В. Скляр

Подход с использованием нотации Claim-Argument-Evidence (CAE) является одной из методик для поиска проблем в разработке информационно-управляющих систем для последующего подтверждения соответствия регулирующим требованиям. Предложен новый подход для развития методологии Assurance (Security and Safety) Case в виде проектирования на основе Assurance Case (Assurance Case Driven Design, AC DD). Практическое использование AC DD заключается в повышении эффективности процесса сертификации и лицензирования. В статье предложены общий процесс для AC DD, а также подход к развитию нотации CAE.

Ключевые слова: Assurance Case, жизненный цикл безопасности, Claim-Argument-Evidence.

ПРОЕКТУВАННЯ НА ОСНОВІ ASSURANCE CASE ДЛЯ СИСТЕМ З ВИКОРИСТАННЯМ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА МОВ ОПИСУ АПАРАТУРИ

В. С. Харченко, В. В. Скляр

Підхід з використанням нотації Claim-Argument-Evidence (CAE) є одною з методик для пошуку проблем у розробці інформаційно-управляючих систем для подальшого підтвердження відповідності регулюючим вимогам. Запропоновано новий підхід для розвитку методології Assurance (Security and Safety) Case у вигляді проектування на основі Assurance Case (Assurance Case Driven Design, AC DD). Практичне використання AC DD полягає у підвищенні ефективності процесу сертифікації та ліцензування. У статті запропоновано загальний процес для AC DD, а також підхід до розвитку нотації CAE.

Ключові слова: Assurance Case, життєвий цикл безпеки, Claim-Argument-Evidence.

Харченко Вячеслав Сергеевич – д-р тех. наук, проф., зав. каф. компьютерных систем и сетей Национального аэрокосмического университета им. Н. Е. Жуковского «ХАИ», Харьков, Украина, e-mail: V.Kharchenko@khai.edu.

Скляр Владимир Владимирович – д-р техн. наук, проф., проф. каф. компьютерных систем и сетей Национального аэрокосмического университета им. Н. Е. Жуковского «ХАИ», Харьков, Украина. e-mail: vvsklyar@ukr.net.

Kharchenko Vyacheslav – Doctor of Science, Professor, Head of Department of Computer Systems and Networks of National Aerospace University named by N. Ye. Zhukovskiy "KhAI", Kharkiv, Ukraine, e-mail: V.Kharchenko@khai.edu.

Sklyar Vladimir– Doctor of Science, Professor, Professor of Department of Computer Systems and Networks of National Aerospace University named by N. Ye. Zhukovskiy "KhAI", Kharkiv, Ukraine, e-mail: vvsklyar@ukr.net.