Andrzej Białas
Barbara Flisiuk

Institute of Innovative Technologies EMAG

SPECIALIZED DEVELOPMENT ENVIRONMENTS FOR SECURITY-ENHANCED IT PRODUCTS AND SYSTEMS

Introduction

The paper concerns the issue how to organize specialized development environments for IT products which are to be used in high-risk operational environments. The security measures for such products have to be reliable in order to work properly in critical situations. A development environment is understood here as a technical and organizational solution with a certain objective and tasks, placed in a certain physical environment of the institution, properly organized, equipped and protected.

The EMAG Institute has completed a project CCMODE (Common Criteria compliant Modular Open IT security Development Environment) [CCMODE]. The results of the project enable to build development environments for IT products which need reliable security measures. In such environments it is possible to develop IT products accompanied with a special type of documentation, called evaluation evidences. The developed product and its documentation are submitted for evaluation to an independent accredited laboratory.

The CCMODE project concerns creative implementation of the international standard ISO/IEC 15408 Common Criteria for Information Security Evaluation (CC) [CC1-3, CEM, CCPortal, Hig10, SC07, Her03]. The standard enables to develop IT products (hardware, software, systems) whose security measures can be trusted, i.e. they can be applied in responsible, high-risk projects.

In the course of the project there was extensive research conducted on the state of the art of available technologies in this respect. The research results confirmed that:

- there are no evaluation evidence patterns; moreover, the evidences submitted for evaluation with the IT product are usually prepared by external consultants whose services are quite costly for developers,

- there are only few tools available to support the Common Criteria methodology; they are limited to the very first stage of the process, i.e. the preparation of the so called Security Target,
- there are very few attempts to make data bases for developers and the use of ontologies is scarce,
- the use of security information standards for the protection of development environments has been consistently seen as a challenge,
- an innovative concept of "site certification", related to the certification of development environments, has had only few implementations so far and still remains in the phase of experiments.

These factors are barriers against wider dissemination of the standard whose application is commonly believed to be difficult and expensive. This has become motivation to take up the CCMODE project. The project resulted in the following products:

- patterns for constructing the elements of a development environment, including patterns of evaluation evidences,
- a method to implement patterns while constructing the environment,
- software which makes use of technologies, supports the environment implementation process, and manages this environment during its exploitation – CCMODE Tools,
- know-how necessary to implement and exploit the environment.

CCMODE products have been developed to address the needs of developers, who produce hardware, software and systems, and the needs of the products users. In order to present, improve and exploit CCMODE products, there was a laboratory organized in the EMAG Institute – SecLab, where security enhanced IT products can be developed. This laboratory is the subject of this paper. Additionally, the authors presented the standards on which SecLab's functioning is based, its organization, tools used to develop IT products, methods applied to protect data related to the projects carried out in SecLab, and examples of completed projects.

Basic standards

The organization and procedures of the SecLab laboratory are in compliance with the requirements of ISO/IEC 15408 Common Criteria, while the security of information and development processes is provided by an integrated system for information security and business continuity management, according to ISO/IEC 27001 and BS 25999 (ISO 22301).

The reliability issue of security measures is solved by reference to the CC standard [CC1-3]. It is assumed there that the reliability of security measures depends on how thoroughly and with how much rigour these measures are designed, tested, verified, documented, etc. Thus our confidence in the IT product depends on the degree of the rigour, the use of best engineering practices and good organization of the development-, production- and maintenance environment of the product. In CC, the term reliability has been replaced by a more precise one: assurance.

The name assurance points at another aspect of this term – independent evaluation leading to the certification of IT products equipped with certain security measures. Assurance can be measured by means of Evaluation Assurance Levels (EAL) in the range from EAL1 (min.) to EAL7 (max.). The applied degree of rigour impacts the cost of the product development, production and maintenance. That is why, when an EAL for the product is declared, it is vital to compromise between the costs and the chosen EAL. In practice, among over one thousand CC-certified IT products, the majority are those with EAL3 and EAL4. An IT product, in the nomenclature of the standard, is called Target of Evaluation (TOE).

The CC methodology comprises three basic processes:

- IT security development process; after different security analyses there is a document prepared, called Security Target (ST); ST is a set of security requirements, i.e. functional requirements which describe how the security measures should work and assurance requirements which determine how much assurance we can have in them;
- TOE development process, including the preparation of TOE documentation; this documentation, being an extension of the Security Target, is in fact evaluation evidence made for the purposes of the security evaluation process;
- security evaluation process carried out in an independent, accredited laboratory in a country which has its own evaluation scheme, i.e. which implemented the standard and signed the Common Criteria Recognition Arrangement (CCRA) [CCPortal].

The security of the development environment is an important issue here. The CC standard stipulates certain requirements in this respect (assurance family ALV_DVS [CC1-3]/part 3). It was assumed that in SecLab, which plays a role of such an environment, the protected information will be this about projects and technologies, and about methods for implementing security measures embedded in IT products (cryptographic, access control, information exchange mechanisms, transactions, accountability, non-repudiation, etc.).

The requirements of the ALV_DVS family are quite basic and do not address sufficiently the maintenance of the assumed level of security. Therefore, it is common to have an ISMS (Information Security Management System) implemented in the development environment, according to ISO/IEC 27001. ISMS can be supplemented by BCMS, i.e. Business Continuity Management System according to BS 25999 (ISO 22301). The latter is more important for the production process than for the development one.

Both systems were implemented in SecLab as one integrated system. The requirements of the Quality Management System (QMS) according to ISO 9001 were taken into account too, as QMS has been functioning in EMAG for years.

SecLab – purpose and organization

The SecLab laboratory for the development of security-enhanced IT products has two basic tasks:

- it provides its resources to the developers for the purpose to develop security-enhanced IT products,
- it deals with demonstration and dissemination of the developed solutions, offers training and workshops.

SecLab was placed in a suitable room of the Institute and equipped with proper tools to conduct R&D works. Obviously, there were proper measures provided to ensure its security.

It was assumed that SecLab would carry out projects up to EAL4+, according to the CC standard.

SecLab deals with the IT product from the idea, to the prototype and its documentation.

The operations of the laboratory include: design of hardware and software, making models and prototypes of hardware and software (including firmware), testing models and prototypes, integration of systems, testing and validation of the developed solutions.

It is possible to use different models of the products life cycles, while within a given model only selected phases can be taken into account.

The following development phases were assumed for an intelligent device:

1. Documentary evidence of the idea or a client's order.
2. Preparing the design and its technical documentation.
3. Making a model, preparing documentation for tests and verification.
4. Making a prototype, conducting functional and environmental tests and validation.
5. Submitting the product documentation to an external unit dealing with production, sale and maintenance services.

The following phases were assumed for software development:

1. Initiation (plan, budget, resources, etc.).
2. Specification of requirements.
3. Design (preparing models with degree of detail enough to enable their implementation).
4. Implementation and preliminary testing of the program module.
5. Integration (connecting modules into larger structures which make a system).
6. Validation (verification whether the produced system meets the requirements of the client/user listed in the specification).
7. Installation (implementation of the produced system in its operational environment).

SecLab has two organizational sections:

- operational section responsible for projects execution,
- security section.

For the operational section the following sample roles can be distinguished:

- project manager who initiates, organizes and supervises the project of a concrete IT product;
- designer who identifies requirements and functional assumptions, makes models of the product, supervises the preparation of documentation in the whole course of the project;
- programmer who makes algorithms and implements them as program codes, prepares software documentation,
- electronic engineer who prepares schemes and requirements for printed circuits;
- mechanic engineer who designs mechanical elements and other elements of the software, documents and assembles models and prototypes;
- tester who prepares functional tests and other tests for the software, prepares testing documentation.

For the security section the following sample roles can be distinguished:

- security officer responsible for the security of development processes and the related data,
- analyst who deals with data analysis and risk analysis in the scope of the information security management system (ISMS) of SecLab,
- auditor authorized to carry out internal audits of ISMS,
- incidents coordinator who coordinates incidents reported from SecLab and reacts to changes caused by these incidents.

The SecLab team are permanent employees (engaged in the maintenance of the laboratory) and temporary employees (engaged in particular projects or performing particular tasks there).

SecLab specialized equipment

SecLab was equipped with an independent network infrastructure with servers, connected with EMAG's infrastructure and the outside. The laboratory has stands for the development of intelligent hardware and firmware and stands for the development of software.

Apart from typical tools for electronic engineers (electronic schemes editor, simulator, oscilloscope, etc.), programmers (software development tools) and office software, SecLab was equipped with CCMODE products.

The developer of an IT product should submit the product for evaluation with its evaluation evidences. The range of the evidences is partly equivalent to typical project documentation. Yet, some specific elements are needed to prove that the product meets the requirements of the declared EAL. The degree of detail and the volume of the evidence depend on this declared EAL. The evidence can be typical documentation (e.g. administrator's manual, installation procedures), can be the result of independent investigations or observations (e.g. testing report, list of risks, vulnerability analysis report), or a document confirming one's behaviour (confirmation that a certain procedure is used, acceptance protocol of certain activities, different records).

IT security developers find it difficult to work out such evaluation evidences and often have to use expensive services of consultants [Hig10]. Therefore the patterns of evaluation evidences were prepared within the CCMODE project. Using these patterns, the developer can focus on the product as such and does not have to worry about the form of the evidence, its coherence and consistence with other pieces of evidence, completeness, compliance with the standard, etc. Besides, the developer gets hints how to prepare evidence on the basis of the pattern. The patterns were prepared for evidences related to all assurance components from the third part of Common Criteria [CC1-3], in a different manner for all possible EALs [Bia10, Bia11a]. The basics of the CC methodology can be found in [Bia11b, Bia12].

In SecLab the patterns of evidences have a form of MS Word® templates with hints that help to fill the templates with contents about the developed product. Thus, after the template is filled it automatically becomes evaluation evidence.

Extra benefits resulted from the implementation of patterns in the CCMODE Tools knowledge base. Some patterns subscribe to the concept of "site certification" which allows to certify a development environment with a view to develop many products there, under the same site certificate, and thus reduce evaluation and certification costs [RogNow12].

The first group of patterns concerns documents which describe basic security requirements:

- Security Target pattern (STp) – Structure and content of the Security Target of the TOE;
- low assurance Security Target pattern (laSTp) – Structure and content of a simplified ST document of the TOE (used for EAL1);
- Protection Profile pattern (PPp) – Structure and content of the Protection Profile of the TOE;
- low assurance Protection Profile pattern (laPPp) – Structure and content of a simplified PP document of the TOE (used for EAL1);
- Site Security Target pattern (SSTp) – Structure and content of the Site Security Target (SST) document for the development environment, according to the AST class (Site Security Target Evaluation); the basis for the "site certification" concept.

The Security Target pattern (STp) is the basis of the IT security development process.

The second group of patterns describes how the development environment is organized for particular EALs:

- Life-cycle model definition pattern (ALC_LCDp) – describes the TOE life cycle and defines the structure of the whole development environment.
- Development security pattern (ALC_DVSp) – presents physical, procedural, human and other security measures which can be used in the development environment to protect the TOE and its parts; the ISMSp pattern can be used optionally, as a source of extra assurance.
- Configuration management (CM) capabilities pattern (ALC_CMCp) – defines detailed description of the configuration management system (CMS); enforces discipline and control in the specification and modification processes of the TOE and the related information.
- Configuration management scope pattern (ALC_CMSp) – presents configuration lists and their elements which are managed in the CMS system.
- Tools and techniques pattern (ALC_TATp) – defines the method of describing control tools, their options and techniques used in the development environment (e.g. programming languages, documentation, implementation standards, runtime libraries).

- Delivery pattern (ALC_DELp) – describes how to deliver safely the ready TOE from the development environment to the user.
- Flaw remediation pattern (ALC_FLRp) – presents requirements for the developer to track and correct the flaws; optional for any EAL.
- Information Security Management System pattern (ISMSp) – is, actually, a set of patterns for the implementation of the ISMS, according to ISO/IEC 27001, in the development environment. This option is proposed in CCMODE for even better protection of the project data.

The third group of patterns shows how to specify IT products developed in the development environment:

- Security Architecture pattern (ADV_ARCp) – presents the description of architecture in which TOE security functions (TSFs) are implemented; this specification is to prove that the functions are protected thanks to the proper use of the architecture properties;
- Functional specification pattern (ADV_FSPp) – presents TOE security functions interfaces (TSFIs), which contain measures available to the users and enabling to use these functions;
- TOE design pattern (ADV_TDSp) – with respect to the used EAL, the pattern presents the TOE decomposition into subsystems and modules; it provides context for the description of TOE security functions and describes these functions;
- Implementation representation pattern (ADV_IMPp) – presents the representation method of TOE security functions (source codes for the software, electronic diagrams, binary files, codes in the hardware description language, etc.);
- TSF internals pattern (ADV_INTp) – presents the method for assessing the internal structure of security functions; functions with organized internal structure are easier to implement, have fewer flaws and vulnerabilities;
- Security policy modelling pattern (ADV_SPMp) – provides extra assurance which results from the formal model of the security policy of TSFs;
- Preparative procedures pattern (AGD_PREp) – presents how to install the TOE and prepare it for work in the operating environment;
- Operational user guidance pattern (AGD_OPEp) – shows how to prepare instructions and manuals for all types of TOE users in the evaluated configuration;
- Functional tests pattern (ATE_FUNp) – enforces proper specification, performance and documentation of tests;
- Test Coverage pattern (ATE_COVp) – helps to demonstrate that the TSFIs are properly covered by tests;
- Test Depth pattern (ATE_DPTp) – helps to demonstrate that particular TOE subsystems and modules are properly covered by tests;

- Independent testing pattern (ATE_INDp) – has an auxiliary character because the ATE_IND evaluation evidence is worked out by the evaluators; the pattern is used to verify the developer's tests and additional tests conducted by the evaluator.

There is one more pattern:

- Vulnerability analysis (AVA_VANp) – concerns the vulnerability analysis and is prepared for the AVA_VAN family.

This pattern refers partly to the environment, partly to the IT product. It takes into account the fact that environmental vulnerabilities may be transferred into the product.

Development patterns, which are one of the SecLab pillars, are described in detail in [Bia11b], while their implementations – in the further presented CCMODE Tools in [Bia12].

Figure 1 features a sample pattern presenting a Site Security Target (SST). More specifically, its section referring to the Security Problem Definition (SPD) [Bia11b]. The SSTp pattern has a structure similar to STp. However, the former refers to the security of the "site", and the latter to the security of the IT product. The SPD section describes resources protected in the environment and subjects of this environment, including threat agents, threats as such, assumptions and Organizational Security Policies (OSPs). The problem is solved by specified security objectives. On the left side of the figure there is the structure of the pattern. On the right one can see fields which are to be filled with content about the performed project (here: SPD section). Using this pattern, the developer or security analyst can focus on the content which is put into proper fields according to the hints (see the right bottom corner of the Figure 1). The hints tell the developer what to do and how, sometimes they even prompt phrases. The SSTp pattern is quite untypical as it concerns a relatively new concept of the environment organization, called "site certification". This concept is presented in CCMODE along with the traditional approach. Site certification assumes that the whole environment will be certified. This way many similar products can be developed there with no need to evaluate the environment-related evidences (ALC class [CC1-3]) over and over again. The Security Target pattern (STp) for the product and the Protection Profile pattern (PPp) have similar structures, however, they do not have the so called TOE Security Functions (TSFs).

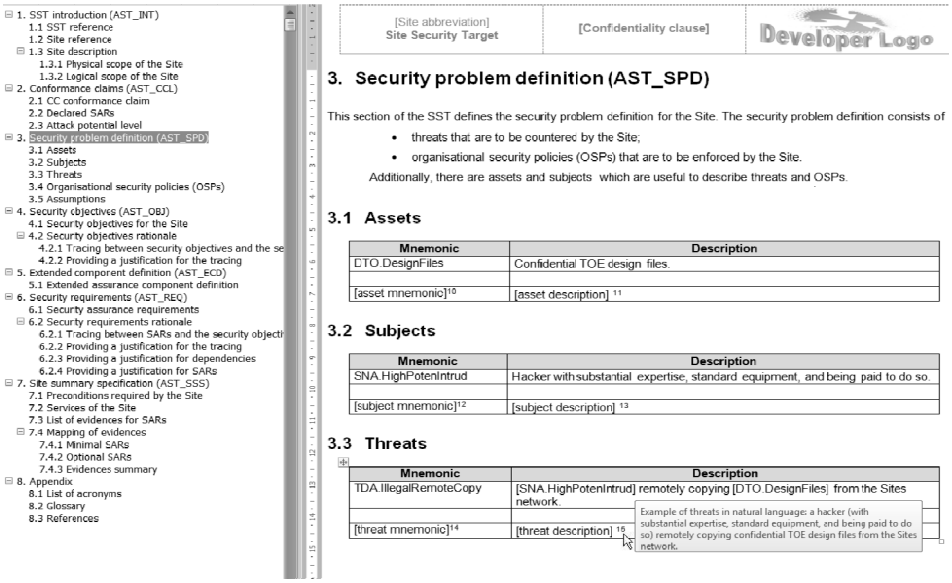

Fig. 1. Site Security Target pattern filled with contents expressing the Security Problem Definition

Source: EMAG Institute.

The patterns are important elements of the SecLab laboratory – they represent the know-how of security consultants. More benefits, similarly to those derived from CAD/CAM/CAE systems, can be obtained thanks to the application of the CCMODE Tools software which makes use of knowledge engineering.

The basic tool of SecLab is the CCMODE Tools software which supports the development of IT products in compliance with ISO/IEC 15408. CCMODE Tools consists of the following modules, some of which were developed in the EMAG Institute:

- EMT Environment Management Tool – the basic application which supports the project management and integrates other modules and external systems;
- GenDoc – generator of evaluation evidence documents on the basis of the implemented patterns;
- EA-plugin to Enterprise Architect® made by Sparx – for conducting analyses and making semiformal security models; TOE decomposition into subsystems and modules; test coverage of TOE interfaces, subsystems and modules; the results of the analyses with rationales are transferred to evaluation evidences by means of the GenDoc application;
- QUIZ – assessment of the environment compliance with the declared EAL; assessment of evaluation evidences according to CEM [CEM] (i.e. CC evaluation methodology);

- knowledge base – for the exchange of information between particular elements of CCMODE Tools; it comprises structured knowledge contained in Common Criteria and CEM, documentation patterns, transformation methods, vocabulary data of the system modules, patterns of life cycle models, i.e. common data for all projects; it also comprises data produced within particular projects which are reflected in the developed evaluation evidences;
- integrated external systems (developed outside EMAG):
  - Enterprise Architect® – for modelling and designing in the UML language; apart from the EA plugin for conducting projects, particularly software projects, one can use all possibilities of the EA system;
  - TestLink – system for tests management: test plans, test scenarios, tests performance, testing teams;
  - Redmine – system for the management of security flaws reported in the course of the project by testers, or after the project completion by the TOE users;
  - SVN (Subversion) – system for maintaining the state of data sources and documentation, as well as the state of the development environment; the basis for configuration management in the whole system;
  - LDAP/AD (Lightweight Directory Access Protocol/Active Directory) – for the management of user accounts of the whole CCMODE Tools system.

Within the CCMODE project there was a huge amount of knowledge accumulated about the development of security-enhanced IT products and the use of the CC standard. This knowledge is available in the knowledge base of the tool.

Information security and protection of development processes in SecLab

The SecLab laboratory makes use of the OSCAD system which has been developed within a project financed by Poland's National Centre for Research and Development and the EMAG Institute. OSCAD is a computer-aided, integrated system for the management of information security (ISO/IEC 27001) and business continuity (BS 25999). In SecLab this system is responsible for:

- monitoring factors which breach information resources and continuity of business processes,
- reducing consequences of such events and supporting recovery after incidents,
- managing information related to SecLab (resources, processes, roles),
- managing incidents, tasks and security documentation in SecLab,
- collecting information from external systems (ERP, physical protection and fire protection systems).

Detailed information about OSCAD can be found in [OSCAD, Bia11c].

The implementation of OSCAD included the following operations:

- preparation of the system vocabulary and loss matrix,
- identification of roles, protected assets and processes,
- preparation of Information Security Policy for SecLab and related procedures,
- general and detailed risk analysis, selection of suitable security measures,
- development of an incidents management subsystem and efficiency measures subsystem,
- audits and other activities required by standards.

Sample projects carried out in the laboratory

In the SecLab laboratory, within the CCMODE Tools validation, there were evaluation evidences prepared for two products:

- complex software, i.e. the OSCAD system supporting information security and business continuity management [Bia12]/chapter 9,
- intelligent sensors for monitoring security parameters in the mining industry: gas monitoring sensor with a multi-purpose measuring head (MCX), dust meter (PŁ-2), and temperature increase sensor (CPT) [Bia12]/chapter 8.

SecLab – conclusions

The paper describes the experimental implementation of the CCMODE project results in the EMAG Institute. They were implemented in the form of a laboratory for the development of security-enhanced IT products – SecLab.

The authors presented the purpose, organization and equipment of the laboratory, along with the projects conducted there. Additionally, they discussed the methods to protect the project data and development processes, based on information security and business continuity management standards.

In SecLab it is possible to perform any kind of IT projects according to the CC methodology. The laboratory is equipped with suitable tools and security measures. It can serve as a demonstration laboratory for different technologies and can be used for the following:

- R&D works in the realm of security,
- consulting and training,
- supporting businesses which implement their own development environments in compliance with Common Criteria,
- demonstration projects of different IT products which are particularly dependent on security,
- promotion of best practices in IT products development.

This paper is an introduction to [BiaFli14, Bia14]. These two publications extend the topic and present a more formal approach to the processes of developing IT products with declared EALs. They also discuss shortly the processes of the integrated ISMS/BCMS which is responsible for the security of development processes in SecLab.

References

[Bia14] Białas A.: Common Criteria Compliant IT Product Development in the Experimental SecLab Laboratory. In: M. Pańkowska, J. Palonka, H. Sroka (eds.): Ambient Technologies and Creativity Support Systems. Uniwersytet Ekonomiczny, Katowice 2014.

[Bia11c] Białas A.: Computer Support in Business Continuity and Information Security Management. In: A. Kapczyński, E. Tkacz, M. Rostański (eds.): Internet – Technical Developments and Applications 2. „Advances in Intelligent and Soft Computing" 2011, Vol. 118, Springer-Verlag, Berlin-Heidelberg, pp. 129-144.

[Bia12] Białas A. (ed.): Komputerowe wspomaganie procesu rozwoju produktów informatycznych o podwyższonych wymaganiach bezpieczeństwa (Computer Support for the Development of IT Products of Enhanced Security). Wydawnictwo Instytutu Technik Innowacyjnych EMAG, financed by UE POIG 1.3.1, Katowice 2012.

[Bia10] Białas A.: Patterns-based Development of IT Security Evaluation Evidences. The 11th International Common Criteria Conference, Antalya, 21-23 September 2010 (published in an electronic version), http://www.11iccc.org.tr/presentations.asp.

[Bia11a] Białas A.: Patterns Improving the Common Criteria Compliant IT Security Development Process. In: W. Zamojski, J. Kacprzyk, J. Mazurkiewicz, J. Sugier, T. Walkowiak (eds.): Dependable Computer Systems. „Advances in Intelligent and Soft Computing" 2011, Vol. 97, Springer-Verlag, Berlin-Heidelberg, pp. 1-16.

[Bia11b] Białas A. (ed.): Zastosowanie wzorców projektowych w konstruowaniu zabezpieczeń informatycznych zgodnych ze standardem Common Criteria (Design Patterns for the Development of IT Security in Compliance with Common Criteria). Wydawnictwo Instytutu Technik Innowacyjnych EMAG, financed by UE POIG 1.3.1, Katowice 2011.

[BiaFli14] Białas A., Flisiuk B.: IT Security Development Process in the Experimental SecLab Development Environment. In: M. Pańkowska, J. Palonka, H. Sroka (eds.): Ambient Technologies and Creativity Support Systems. Uniwersytet Ekonomiczny, Katowice 2014.

[CCMODE] CCMODE (Common Criteria compliant, Modular, Open IT security Development Environment). http://www.commoncriteria.pl/, 2014.

[CEM] CEM v3.1, Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, http://www.commoncriteria.portal.org/, 2009.

[CC1-3] Common Criteria for IT Security Evaluation, part 1-3. v. 3.1.2009.

[CCPortal] Common Criteria Portal. http://www.commoncriteriaportal.org/, 2014.

[Her03] Hermann D.S.: Using the Common Criteria for IT Security Evaluation. CRC Press: Boca Raton, FL, USA, 2003.

[Hig10] Higaki W.H.: Successful Common Criteria Evaluation. A Practical Guide for Vendors. Copyright 2010 by Wesley Hisao Higaki, Lexington, KY 2010.

[OSCAD] OSCAD website. http://www.oscad.eu, 2014.

[RogNow12] Rogowski D., Nowak P.: Pattern Based Support for Site Certification. In: W. Zamojski et al. (eds.): Complex Systems and Dependability. „Advances in Intelligent and Soft Computing (AISC)" 2012, 170, pp. 179-193, Springer-Verlag, Berlin-Heidelberg.

[SC07] Site Certification. Supporting Document Guidance, version 1.0, revision 1 (CCDB-2007-11-001), October 2007, http://www.commoncriteriaportal.org/ (accessed on February 26, 2014).

SPECJALIZOWANE ŚRODOWISKA ROZWOJU DLA SYSTEMÓW I PRODUKTÓW INFORMATYCZNYCH WYSOKO ZABEZPIECZONYCH

Streszczenie

Artykuł zawiera odpowiedź na pytanie, jak organizować specjalne środowiska rozwoju produktów informatycznych, które mają być użyte w środowiskach operacyjnych wysokiego ryzyka. Środki bezpieczeństwa dla tych produktów muszą być wiarygodne w celu umożliwienia właściwej pracy w krytycznych sytuacjach.

Środowisko rozwoju jest rozumiane jako rozwiązanie organizacyjno-techniczne o określonych celach i zadaniach, umieszczone w pewnym środowisku fizycznym instytucji, odpowiednio zorganizowane, wyposażone i chronione. Przedmiotem badań autorów jest laboratorium SecLab. Autorzy przedstawiają standardy funkcjonowania laboratorium SecLab, jego organizację, narzędzia stosowane dla rozwoju produktów informatycznych, metody zastosowane dla ochrony danych związane z projektami realizowanymi w laboratorium SecLab i przykłady zakończonych projektów.