Computing, Telecommunication and Control, 2021, Vol. 14, No. 4, Pp. 71–83.
Информатика, телекоммуникации и управление. 2021. Том 14, № 4. С. 71–83.

Research article
DOI: https://doi.org/10.18721/JCSTCS.14407
UDC 004.05

ENSURING CONFIDENCE IN CONTROL SYSTEMS OF TECHNOLOGICAL EQUIPMENT

A.A. Zelensky[1] ✉, *M.S. Morozkin*[2], *A.N. Panfilov*[3], *V.R. Kuptsov*[4], *A.A. Gribkov*[5]

[1,2,3,4,5] Moscow State University of Technology "STANKIN", Moscow, Russian Federation

✉ zelenskyaa@gmail.com

Abstract. The article considers a complex problem of providing confidence in the used control systems of technological equipment, developed in Russia in conditions of technological backwardness and high dependence on imports of complete control systems, their components and software. A methodology for the system representation of confidence in technological equipment control systems, based on the description of confidence in the system comprising confidence in its constituent quasi-autonomous elements, is investigated. The authors disclose a sequence of quantitative assessment of confidence, determined from the confidence in the results of the development and testing of control systems, their components and software from the viewpoint of functional reliability and information security. Possibilities of increasing confidence in control systems are considered, and the problem of providing functional reliability and information security is analyzed. As part of the study of the problem of information security of control systems of technological equipment, threats associated with vulnerabilities and malware are considered. In addition, the study systematizes undocumented features and considers methods for their detection.

Keywords: trust, functional reliability, information security, testing, undocumented features, vulnerabilities, software and hardware implementations

Acknowledgements: The study was carried out with the financial support of the Ministry of Science and Higher Education of the Russian Federation within the framework of the state task (Project No. FSFS-2020-0031)

Citation: Zelensky A.A., Morozkin M.S., Panfilov A.N., Kuptsov V.R., Gribkov A.A. Ensuring confidence in control systems of technological equipment. Computing, Telecommunications and Control, 2021, Vol. 14, No. 4, Pp. 71–83. DOI: 10.18721/JCSTCS.14407

Научная статья
DOI: https://doi.org/10.18721/JCSTCS.14407
УДК 004.05

ОБЕСПЕЧЕНИЕ ДОВЕРИЯ К СИСТЕМАМ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКОГО ОБОРУДОВАНИЯ

А.А. Зеленский[1] ✉, *М.С. Морозкин*[2], *А.Н. Панфилов*[3], *В.Р. Купцов*[4], *А.А. Грибков*[5]

[1,2,3,4,5] Московский государственный технологический университет "СТАНКИН", Москва, Российская Федерация

✉ zelenskyaa@gmail.com

Аннотация. Рассмотрена комплексная проблема обеспечения доверия к используемым системам управления технологического оборудования, сложившаяся в России в условиях технологического отставания и высокой зависимости от импорта комплектных систем управления, их комплектующих и программного обеспечения. Изучена методология системного представления доверия к системам управления технологического оборудования, основанная на описании доверия к системе исходя из доверия к составлявшим её квазиавтономным элементам. Раскрыта последовательность количественной оценки доверия, определяемой из доверия к результатам разработки и тестирования систем управления, их комплектующих и программного обеспечения с точки зрения функциональной надежности и информационной безопасности. Рассмотрены возможности повышения доверия к системам управления, проведен анализ проблемы обеспечения функциональной надежности и информационной безопасности. Изучены угрозы, связанные с уязвимостями и вредоносными программами. Систематизированы недекларированные возможности, описаны методы их выявления, проведена оценка текущего состояния организационной системы для выявления недекларированных возможностей в России.

Ключевые слова: доверие, функциональная надежность, информационная безопасность, тестирование, недекларированные возможности, уязвимости, программная и аппаратная реализации

Финансирование: Исследование выполнено при финансовой поддержке Министерства науки и высшего образования РФ в рамках государственного задания (проект NoFSFS-2020-0031)

Для цитирования: Zelensky A.A., Morozkin M.S., Panfilov A.N., Kuptsov V.R., Gribkov A.A. Ensuring confidence in control systems of technological equipment // Computing, Telecommunications and Control. 2021. Т. 14, № 4. С. 71–83. DOI: 10.18721/JCSTCS.14407

Introduction

The basis of the country's industrial development is the formation and renewal of fixed production assets. From 50 to 70 % of the assets cost falls on technological equipment. Along with equipping industry with the necessary technological equipment, a significant task is also to achieve technological security and defense capability of the country.

A prerequisite for solving this problem is to ensure trust in technological equipment, first of all, in control systems, which are the most technologically advanced part of the equipment and the main object of information security threats.

According to GOST R 54583-2011 "Methods and means of ensuring security. Fundamentals of trust in information technology security. Part 3 – Analysis of trust methods", the purpose of ensuring trust is to create confidence in the reliable functioning of the product under specified conditions.

To ensure this trust, the control system of technological equipment must have [1]:

– functional reliability, i.e. the ability to perform its functions with a given error and repeatability;

– information security, i.e. to ensure the fulfillment of the conditions for maintaining a given level of confidentiality, availability and integrity of information stored, transmitted, received and processed by the system during its operation.

The task of ensuring trust in the control system of technological equipment can be fully solved only on the basis of the development of the entire complex of necessary technologies (from information technology and electronics to mechanical engineering and the production of functional materials) at domestic enterprises certified in the field of information security. The limited scientific and technical potential available in Russia does not yet allow such a solution to be implemented.

In conditions of technological backwardness of the country, the goal of ensuring functional reliability is often achieved through the widespread use of imported electronic components and software, while domestic components and software products are created using foreign equipment and software.

This practice contradicts the requirement formulated by us to ensure trust: a control system for technological equipment of foreign manufacture or built from foreign components and using foreign software cannot guarantee information security (confidentiality, availability and safety of information). The reason for this is the inability to reliably evaluate the control system of technological equipment from the outside, without full access to its hardware and software, which is not provided in practice for imported control systems, their components and programs in the vast majority of cases.

In addition, while ensuring the functional reliability of the control systems of technological equipment due to imports, in fact, the long-term reliability of the systems is not guaranteed. It can be eliminated by factors of global competition with companies and countries-suppliers of control systems, components and software by stopping the supply of spare parts, maintenance, etc. by means of unfair competition.

The purpose of this study is to substantiate and formalize the problem of ensuring trust in the control systems of technological equipment. To do this, it is necessary to solve two main tasks:

– to develop a methodology for quantifying trust in control systems based on a set of indicators characterizing functional reliability, information security and available for practical determination;

– to analyze the current state, development trends and the main technical and organizational problems of achieving confidence in the functional reliability and information security of control systems.

The solution of these tasks will make it possible to determine the key components of trust in control systems, as well as the means and practical possibilities of ensuring them now and in the future.

Trusted control system

A necessary condition for the development and assessment of trust in control systems is the availability of a methodology for quantifying the level of trust. An analysis of existing works in the field of assessing trust in control systems [2–4, etc.] shows that such a methodology does not currently exist. Therefore, the authors of this article have developed an original methodology based on data available for analysis and applicable for practical use. Consider this technique.

Trust in the control system of technological equipment consists of trust at each of the levels of its technological implementation: at the level of the electronic component base; at the level of devices; at the level of software (system and application).

If we evaluate the level of trust at each of the technological levels quantitatively in the range from 0 to 1, where “0” is a complete lack of trust, and “1” is complete trust, then the integral indicator C of the level of trust in the control system of technological equipment will be calculated by the formula:

$$C = \prod_{i=1}^{4} C_i, \quad (1)$$

where C_i – trust indicators at the level of electronic component base ($i = 1$), at the level of devices ($i = 2$), at the level of system software ($i = 3$), at the level of application software ($i = 4$).

The nature of the dependence (1) is such that if at least one of the technological levels does not ensure trust in the control system (for example, there are software inserts in the system software that create information leakage, or the electronic component base does not ensure compliance with the specified functional properties), then the entire control system does not have trust.

The confidence indicator at each of the technological levels is determined as follows:

$$C_i = C_{i1}C_{i2}, \tag{2}$$

where C_{i1} and C_{i2} – indicators of trust in functional reliability and information security at the i-th technological level.

The confidence indicator C_{ij} to functional reliability ($j = 1$) or information security ($j = 2$) at a given i-th technological level is determined based on the confidence indicators C_{ij}^{E} and C_{ij}^{T} of the results of the development and testing of hardware or software at this technological level of the control system:

$$C_{ij} = C_{ij}^{E} + \left(1 - C_{ij}^{E}\right)C_{ij}^{T}. \tag{3}$$

The meaning of formula (3) is that testing leads to an increase in trust, and the greater the degree of distrust $\left(1 - C_{ij}^{E}\right)$ of the development results, the greater the potential for increasing trust C_{ij} due to testing. If the results of development or testing are completely trustworthy ($C_{ij}^{E} = 1$ or $C_{ij}^{T} = 1$), then $C_{ij} = 1$ (when $C_{ij}^{E} = 1$ testing is not required); if the results of development do not cause any trust $\left(C_{ij}^{E} = 0\right)$, then $C_{ij} = C_{ij}^{T}$ – overall trust is determined by trust in the test results; if there is no trust in the test results $\left(C_{ij}^{T} = 0\right)$, then $C_{ij} = C_{ij}^{T}$ – trust is determined by trust in the development results.

Indicators of confidence in the results of development and the results of testing functional reliability ($j = 1$) or information security ($j = 2$) at a given i-th technological level are determined based on the corresponding indicators of the elements of the control system of technological equipment at this level:

$$C_{ij}^{E} = \sum_{p=1}^{p_{i\max}} \left(C_{ijp}^{E} W_{ijp}^{E}\right), \; C_{ij}^{T} = \sum_{p=1}^{p_{i\max}} \left(C_{ijp}^{T} W_{ijp}^{T}\right), \tag{4}$$

where $p_{i\max}$ – the number of elements of the control system of technological equipment at the i-th technological level (electronic component base, devices, system or application software); C_{ijp}^{E}, C_{ijp}^{T} – indicators of confidence in the result of the development or testing of the p-th element at the i-th technological level according to the j-th requirement (functional reliability or information security); W_{ijp}^{P}, W_{ijp}^{T} – statistical weights $\left(\sum_{p=1}^{p_{i\max}} W_{ijp}^{P} = 1; \; \sum_{p=1}^{p_{i\max}} W_{ijp}^{T} = 1\right)$ of a p-th element at the i-th technological level when evaluating the confidence indicator according to the j-th requirement for the result of development or testing.

The indicator of confidence C_{i1}^{E} in the results of development from the point of view of functional reliability is determined on the basis of an expert assessment, which is influenced by: the status of the company and the country of the developer (scientific and technical level, product quality, business reputation), data on the functional reliability of similar products (the same and alternative developers), a description of the technical characteristics of the product (including documented data on testing during production), etc. Testing as part of development does not mean that testing will no longer be required in the future. During the verification of purchased products, it is necessary, however, when assessing the reliability of subsequent tests, to take into account the documented test results of the development stage, since repeated testing is less informative and contributes less to increasing confidence.

The indicator of confidence C_{i2}^{E} in the results of development from the point of view of information security is determined on the basis of expert assessment and depends on the reputation of the developer

(whether violations of information security were detected earlier), as well as on the availability of Russian certification in the field of information security for the (domestic) developer.

The indicators of confidence C_{i1}^{E} and C_{i2}^{T} of the test results from the point of view of functional reliability and information security are determined on the basis of expert assessment and depend on: the testing methods used (for functional reliability or information security) with a known reliability of the results, which is strongly influenced by the "transparency" of the product (availability of access to program code, complete circuits of microprocessors, etc.; the higher the "transparency" of the product, the higher the confidence in the test results); the reputation of the organization performing the testing, including the availability of state licenses for certification tests.

To assess the confidence indicator C_{i2}^{T} to the test results from the point of view of information security, an alternative approach can also be used. In this approach, the confidence indicator is defined as the ratio of detected and undetected vulnerabilities and undocumented features, taking into account their statistical weight set based on the degree of threats to information security created by them. This approach can be applied to widespread systems with standard structural elements, the use of which has collected significant statistics.

The final formula of trust in the control system of technological equipment combines formulas (1–4):

$$C = \prod_{i=1}^{4} \prod_{j=1}^{2} \left(\sum_{p=1}^{p_{i\max}} \left(C_{ijp}^{E} W_{ijp}^{E} \right) + \left(1 - \sum_{p=1}^{p_{i\max}} \left(C_{ijp}^{E} W_{ijp}^{E} \right) \right) \sum_{p=1}^{p_{i\max}} \left(C_{ijp}^{T} W_{ijp}^{T} \right) \right), \quad (5)$$

where C_{ijp}^{E}, C_{ijp}^{T} – indicators of confidence in the results of development and in the results of testing of the p-th element at the i-th technological level according to the j-th requirement; W_{ijp}^{P}, W_{ijp}^{T} – statistical weights of a p-th element at the i-th technological level when assessing the confidence index according to the j-th requirement for development results and testing results.

Functional reliability of control systems

Currently, in Russia, the majority of components for control systems of technological equipment are imported. They are supplied to Russia together with equipment (for example, in the form of CNC (computer numerical controlled) systems installed on imported machines), in the form of separate control systems (for example, in the form of supplies of CNC systems from Siemens, Heidenhain, Fanuc, etc., which are later installed on domestic equipment), or in the form of separate components, from which domestic control systems for technological equipment are assembled in Russia becoming not fully "domestic" Russian manufacturers of CNC systems (Modmash-Soft, Balt-Systems, SPE "Izhprest", etc.) are small companies and occupy an extremely modest position even in the domestic market of Russia. The total volume of sales of domestic CNC systems is about 3.0 thousand sets per year, of which about 75 % goes to the modernization of machine tools [5].

In 2019, the share of imported equipment in the total volume of Russian consumption of CNC technological equipment was 90 %, including metalworking equipment – 92 %, industrial robots – 95 % [5]. More than 90 % of domestic machine tools are equipped with foreign CNC systems, about 85 % of all components of technological equipment control systems are of foreign production [6].

The development of the domestic scientific, technical and production base in the field of hardware and software for control systems of technological equipment is a priority task of the state industrial policy: the global competitiveness of the country significantly depends on solving it. The priorities include the development of the domestic electronic component base[1], as well as the creation of domestic CNC systems for processing equipment[2].

[1] Strategy for the development of the electronic industry of the Russian Federation for the period up to 2030. Approved by the order of the Government of the Russian Federation from 17.01.2020, No. 20-p.

[2] Decree of the Government of the Russian Federation dated 05.11.2020, No. 2869-r "On approval of the Strategy for the development of the machine tool industry for the period up to 2035".

Currently, an urgent task within the framework of ensuring the functional reliability of control systems of technological equipment is the development of competencies in the field of control, testing and research of hardware (digital, analog, digital-analog chips, systems on a chip and other electronic devices) and software.

The methodology of testing electronic devices [7] differs significantly in the case of control at production and in the case of control of a purchased (imported) product.

In the first case, existing methods allow you to check the quality of electronics both during production and at the final stage. As a result, high reliability of the test results is ensured. The main testing methods used in production control [8, 9]: visual automated control (AOI, AXI [10, 11]); in-circuit testing (ICT/FICT), a method based on the contact of probes with the nodes of the assembled board; peripheral scanning (using JTAG [12]); functional testing (FCT); testing after final assembly (EOL) – checking functionality and compliance with the specification.

In the second case, the main control method is an electrical check of the circuit for compliance with the documentation. The most common and low-cost methods of such testing include the nodal impedance measurement method and the peripheral scanning method. The reliability of testing of finished products is currently quite high, although it is somewhat lower than the reliability of testing in the production control process.

In general, it can be stated that the task of testing electronic devices with a reliable result has now been solved, the functional reliability of both domestic and purchased (imported) electronic devices is ensured.

Software testing is a process of research, testing of a software product, aimed at verifying the correspondence between the actual behavior of the program and its expected behavior in a finite set of tests selected in a certain way. Testing of a software product is a mandatory part of its development, and is also carried out as a means of controlling purchased programs.

From the point of view of functional reliability, software testing includes the following main types: system testing (high-level verification of the functionality of the entire system and program), functional testing (testing of the "white" and "black" box), load and stress testing, regression and optimization testing (checking the functionality of the software after making changes or improvements – eliminating bottlenecks), unit testing, interface testing, source code analysis, documentation analysis, etc. [13, 14]. The availability of various types of testing depends on the degree of "transparency" (openness) of the software. The higher the degree of "transparency", the higher the reliability of the test results.

In general, the existing software testing tools make it possible to achieve high reliability of the results and ensure the functional reliability of the software of technological equipment control systems.

Information security of control systems

A wide variety of threats to information security is associated with the use of vulnerabilities, i.e. shortcomings of information system security tools that can be used by the violator (both external and internal) to implement these threats[3]. Among the most common threats associated with vulnerabilities are [15, 16]: unauthorized access of the intruder to the object; illegal use of privileges; hidden channels of information transmission; performing actions by one user on behalf of another; reading deleted data before overwriting and erasing; intentional penetration into the system with unauthorized login parameters; functions not described in the documentation; blocking the system for denial of service to other users; connection to communication lines and introduction into the information system using delay in the actions of a legitimate user; traffic analysis; connection to communication lines and simulation of the system, etc.

Along with threats related to vulnerabilities, significant threats to information security are created by specially created malicious programs [17, 18]: "Trojan horse" (penetrate the system disguised as a legitimate programs, after installation provide the attacker with a wide range of opportunities: espionage, block-

[3] GOST R 53114-2008. Information protection. Ensuring information security in the organization. Basic terms and definitions. Moscow: Standartinform Publ., 2018.

ing work, deactivation of the protection system, etc.); “worm” (programs that are distributed in systems and networks over communication lines; can reproduce themselves without infecting other programs and files); “computer virus” (programs that are capable of infecting other programs, modifying them so that they include a copy of the virus); “greedy program” (programs that capture individual resources of the computer system, preventing other programs or system elements from using them); program bookmarks (program code intentionally entered into the program in order to leak, modify, block, destroy information or destroy and modify the software of the information system and (or) block hardware); “bacteria” and “replicator” (programs that make copies of themselves, overloading memory and processor); “logic” and “time” bombs (programs that block work and destroy data when a certain condition is met or after a given time), etc.

One of the main factors in the emergence of threats to the information security of control systems of technological equipment is the presence of undocumented features (UDF) in them. In relation to the field of computer technology and software (and equipment management systems belong to this field), the following definition is adequate: UDF are the functionality of computer technology and software that are not described or do not correspond to those described in the documentation, which may lead to a decrease or violation of the security properties of information[4].

The analysis of regulatory documents[5] and publications [18] in the field of undocumented features has shown that undocumented features should be classified according to the following main criteria: by reason of their appearance; by technical implementation; by the method of getting into technological equipment; by the nature of activation; by the nature of the threat.

Depending on the reason for the appearance of undocumented features, they are divided into unintentionally introduced, intentionally introduced technological, as well as intentionally introduced with malicious purposes.

Unintentionally introduced undocumented features of the equipment management system are additional functionality not described in the technical documentation. Such additional features may be known to the manufacturer or developer (but are not recognized as significant for the sale of products), or unknown. At the same time, the use of these undocumented features is not expected, although they may create vulnerability of equipment to external threats.

Intentionally introduced technological undocumented features of the equipment control system are additional functionality used by the manufacturer (developer), without expanding the operational capabilities of the equipment or improving its implementation to consumers. Such undocumented features are quite common for both software and hardware.

Any software developer knows that not all the functionality of the program is usually described to the consumer. In particular, the consumer is not given access to control routines (used for debugging and detecting program errors). Some of the functions of the programs can be blocked in case of their unstable operation (in this case, the full functionality is supposed to be implemented in subsequent modified versions of this program). In addition, the program may include a hidden module sending data about its work (for subsequent use of the data to improve the program).

---

[4] GOST R 53114-2008. Information protection. Ensuring information security in the organization. Basic terms and definitions. Moscow: Standartinform Publ., 2018.

[5] Information technology. Methods and means of ensuring security. Criteria for assessing the security of information technologies. Part 1. Introduction and general model (GOST R ISO/IEC 15408-1). Part 2. Functional safety components (GOST R ISO/IEC 15408-2). Part 3. Components of trust in security (GOST R ISO/IEC 15408-3).

Regulations for the inclusion of information about software and hardware vulnerabilities in the data bank of information security threats of the FSTEC of Russia. FSTEC of Russia June 26, 2018

GOST R ISO/IEC 27034-1. Information technology. Methods and means of ensuring security. Application security. Part 1. Overview and general concepts. Moscow: Standartinform Publ., 2015.

GOST R 51275-2006. Information protection. The object of informatization. Factors affecting information. General provisions. Moscow: Standartinform Publ., 2018.

Resolution of the Government of the Russian Federation of 17.11.2007 No. 781 "On approval of the Regulations on ensuring the security of personal data during their processing in personal data information systems".

Similarly, hardware may have functionality that facilitates its maintenance (diagnostics, repair, replacement of blocks, etc.). Often the capabilities of individual elements of equipment are partially blocked. This happens when the equipment control system uses elements (parts, components, modules) that are also used in systems with more functionality.

Undocumented features of the equipment management system introduced for malicious purposes are functionality that serves the interests of the one who introduced them into the management system to the detriment of the interests of the equipment user. The specified damage may constitute unauthorized access to information (on the equipment, its use, its location, etc.), as well as pose a threat to the operation of the equipment. At the same time, in most cases, if these undocumented features are detected, the developers present them as technological ones that serve the interests of the user and improve product quality [19].

An example of the implementation of undocumented features that can be used for malicious purposes is the Intel Management Engine (ME) – an autonomous subsystem built into almost all modern chipsets of Intel processors. It has a firmware that is closed to public access, implemented on a separate microprocessor. Intel ME works with the computer turned off (connected to a battery or other power source), has access to the entire contents of the computer's RAM and out-of-band access to the network interface [20, 21].

The technical implementation of undocumented features is divided into the following main groups: software implementation (in a standard computer numerical controlled (CNC) or a programmable logic controller (PLC)); hardware implementation (in a standard CNC or PLC); hardware implementation by a separate device outside the CNC or PLC.

The software implementation of undocumented features is the formation of additional capabilities of the equipment management system due to the expanded undocumented functionality of the software. An example of such UDF is the Computrace LoJack program from Absolute Software [22]. The program sends geolocation data to a remote server, has the ability to remotely lock the computer or erase information from disks by commands from the servers of the developer company, as well as remote full-featured computer management.

Hardware implementation of undocumented features of the equipment control system is the formation of additional hardware capabilities due to the expanded undocumented hardware functionality by changing the operational properties of standard elements of the equipment control system, or connecting additional modules or devices to the control system. An example of such devices are Broadcom network chips (lines in CM 57xx), which have their own flash memory, RAM and RISC processor [23].

According to the method of getting into the control system of technological equipment, undocumented features of equipment are divided into the following groups: UDF laid down by the manufacturer; UDF added by the supplier or logistics company; UDF installed by the service organization (during service, repair, security measures, etc.); UDF installed by the violator.

According to the activation method, UDF equipment is divided into permanent, self-activated and externally activated.

The permanent undocumented features of the equipment are in effect all the time. They represent additional functionality of the equipment, for some reason not specified by the developer.

Independently activated and externally activated undocumented features are functional properties that are in a "dormant" state until some point in time. Self-activation occurs as a result of a given program: after passing a certain time interval or after some time intervals; with a given change in equipment (involving certain software or hardware functions of the equipment control system, changing its location, etc.). Activation of undocumented features from the outside can be carried out through a network connection, electromagnetic and other external influences [24].

Unintentionally introduced and technologically undocumented features almost always belong to the group of permanent ones. Malicious undocumented features can belong to any of the groups. The method of UDF activation is important in determining ways to counteract malicious UDF.

By the nature of threats to the object of protection, undocumented features of the equipment management system are divided into the following main groups: malicious impact on equipment or personnel; unauthorized collection and transmission of information; changing operating modes, disabling technological and auxiliary equipment at the software or hardware level, etc.

Along with the above-mentioned classifications of undocumented features, an important role also belongs to their ability to adapt, to extend to other equipment systems or other equipment, multiplatformity, etc.

Malicious impact on the equipment can be achieved not only by adding undocumented features (program tabs, hidden programs and functional elements), but also by exploiting vulnerabilities in its management system. These vulnerabilities may be the result of development errors or created intentionally for the purpose of subsequent unauthorized access to information or impact on equipment (up to the termination of its operation). According to the latest FSTEC[6] regulations, when certifying security software, testing laboratories need not only to monitor the absence of UDF, but also to search for vulnerabilities, or security flaws.

One of the most problematic areas are low-level programs, in particular drivers that provide interaction between hardware components of the equipment and the operating system used. Eclypsium specialists [25] have identified vulnerabilities in more than forty drivers (including from ASUS, Toshiba, Intel, Gigabyte, Nvidia and Huawei) that allow you to increase your privileges from the user space level to the kernel level.

Tests to identify vulnerabilities and UDF in software include expert, static, dynamic and manual analysis [26, 27]. Expert analysis is based on documentation research, vulnerability scanning, attack modeling, penetration testing and data visualization [28]. Static analysis provides for the identification of vulnerabilities and UDF based on the results of the analysis of the program code in a mode that does not provide for its actual execution. Dynamic analysis provides for the identification of vulnerabilities and UDF based on the results of code analysis in the mode of its direct execution using: fuzzing [29], analysis of the activity of lightweight processes of program interaction, tracking tagged data and other methods. Manual analysis provides for the identification of vulnerabilities and UDF based on the results of the examination of the source/restored code of the evaluation object based on tracking tagged data, directed manual analysis of code sections and data visualization.

The reliability of the test results for identifying vulnerabilities and UDF largely depends on whether the identified vulnerabilities and UDF are known (confirmed) or new, previously unpublished, the nature of the manifestations of which is unknown in advance [30].

An important area of implementation of information security threats is the software of external hardware modules [31], the testing and protection of which is often given significantly less attention than the main software and hardware. As a result, external hardware modules often become a channel for information leakage.

Hardware vulnerabilities and undocumented features are currently studied to a much lesser extent than software ones. The hardware vulnerabilities that have attracted the most attention in recent years include Meltdown and Spectre processor vulnerabilities [32, 33] related to the implementation of predicative algorithms (extraordinary execution, speculative command processing and branch prediction) in some microprocessors, in particular, manufactured by Intel and ARM architecture. These vulnerabilities allow local applications (a local attacker, when launching a special program) to gain access to the memory used by the operating system kernel (Meltdown vulnerability), or to the contents of the virtual memory of the current application or other programs (Spectre vulnerability).

Threats to the information security of hardware are implemented in the following main areas of attacks [34]:

— attacks on external protocols (USB, Bluetooth, CAN) by installing an additional device, or your own software (firmware) instead of the one used;

[6] Regulations for the Inclusion of information about software and hardware Vulnerabilities in the data bank of information security Threats of the FSTEC of Russia. FSTEC of Russia June 26, 2018.

— attacks on embedded software by obtaining (by connecting the device to the programmer and removing the dump) the microcode recorded in the processor, microcontroller or chip, disassembling it and developing the PLD configuration file, and then identifying vulnerabilities for its subsequent modification and use for their own purposes;

— attacks on the electrical circuit based on the analysis of the electrical circuits of printed circuit boards in order to reverse engineer them for subsequent cloning with the addition of additional malicious functions;

— attacks on the microprocessor, implemented at the chip level, based on the analysis of the chip's response (electricity consumption, radiation, time spent, etc.) to passive attacks that do not affect the operation of the device; using time measurements, taking waveforms of current consumption and electromagnetic activity, you can choose a password, identify a cryptographic algorithm and extract a secret key.

When using cloud technologies for the operation of the equipment management system, the threats to the information security of the hardware increase manifold. The currently available hacking capabilities of embedded systems make the construction of trusted management systems based on them practically unrealizable.

Currently, Russia has not formed an organizational system for monitoring, technological audit and reverse engineering of control systems of technological equipment to identify undocumented features and vulnerabilities. The implementation of measures to identify them is (with rare exceptions) optional and is implemented on the initiative of the industrial enterprises themselves by special organizations that have received licenses to perform this activity from the FSTEC. Inspections initiated by control bodies, including the FSTEC, the FSB or the Ministry of Defense, are extremely limited and do not have any significant impact on the safety of industrial facilities.

A common problem of the regulatory framework for the implementation of measures to protect against threats to information security is the lack of regulations defining the practical means and procedure for the implementation of control measures, including control of industrial facilities, technological equipment, individual systems of technological equipment. In particular, according to the "The Concept of protection of computer equipment and automated systems from unauthorized access to information" guidelines[7], regulatory legal acts, organizational, administrative and methodological documents of the FSTEC of Russia are aimed at classifying objects and presenting requirements for computer equipment and automated systems that are certified by the developer of these objects. As a result, all responsibility for the set of security measures lies with the developer, and the existing FSTEC documents are only partially applicable to control systems of technological equipment: they describe only the requirements for objects without affecting the methods of checks that are specific to various hardware and software control systems of technological equipment.

Since the purpose of certification of an object is to confirm the compliance of its information security system in real operating conditions with the information security requirements established by federal laws of the Russian Federation, regulatory legal acts of the President of the Russian Federation, the Government of the Russian Federation, as well as authorized federal executive authorities (FSTEC of Russia, FSB of Russia, etc.), a program and test methodology is developed for each object in accordance with GOST RO 0043-004-2013. At the same time, in order to carry out the necessary measures, it is necessary to obtain all design and software documentation from the developer of technological equipment, which is difficult to implement in practice, especially when it comes to a foreign developer company.

Conclusion

The goal set in the study has been achieved: the substantiation and formalization of the problem of ensuring trust in the control systems of technological equipment has been given. According to the tasks outlined in the study, the following results were obtained:

[7] The concept of protection of computer equipment and automated systems from unauthorized access to information (Approved by the decision of the State Technical Commission under the President of the Russian Federation dated 30.03.1992).

1. An original methodology for quantifying trust in management systems has been created. According to this methodology, trust is determined in accordance with trust in all its elements at all technological levels (the level of electronic component base, devices, system and application software) in relation to ensuring functional reliability and information security based on the assessment of trust in the results of the development and testing of these elements.

2. The functional reliability of imported electronic devices and software used in control systems of technological equipment is currently ensured at the proper level due to existing testing tools. Domestic production of Russian electronic devices and software has small volumes; the functionality of domestic devices and software is significantly lower than that of imported from the leading countries of the world, which limits the scope of domestic products.

3. The main source of threats to the information security of control systems of technological equipment are undocumented features of hardware and software. At present, an organizational system for identifying undocumented features in Russia is still in its formative stages.

REFERENCES

1. **Sabanov A.** Trusted computer systems as a way to counteract the cyber threats. *Protection of information. Inside*, 2015, No. 3(63), Pp. 17–21. (rus)

2. Department of Defense Trusted Computer System Evaluation Criteria. TCSEC, DoD 5200.28-STD, Dec. 26, 1985. Available: *https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/dod85.pdf* (Accessed: 16.09.2021).

3. **Shalin A.P.** Mekhanizmy formirovaniya doveriya v sisteme otsenki sootvetstviya [Confidence-building mechanisms in the conformity assessment system]. *Kontrol Kachestva Produktsii* [*Production Quality Control*], 2019, No. 4, Pp. 19–23. (rus)

4. **Romanov A.V., Gogolevsky A.S., Neyelova O.N., Sokolova V.A.** Assessment of reliability of special technical systems at the stage of their operation. *Systems. Methods. Technologies*, 2018, No. 4 (40), Pp. 13–19. (rus). DOI: 10.18324/2077-5415-2018-4-13-19

5. **Gribkov A.A., Pivkin P.M., Zelenskii A.A.** State industrial policy and the machine-tool industry. *STIN*, 2021, No. 1, Pp. 2–6. (rus). DOI: 10.3103/S1068798X21040092

6. **Kalyayev I.A., Melnik E.V.** Doverennyye sistemy upravleniya [Trusted control systems]. *Mekhatronika, Avtomatizatsiya, Upravleniye* [*Mechatronics, Automation, Control*], 2021, Vol. 22, No. 5, Pp. 227–236. (rus)

7. **Grout I.A.** *Integrated circuit test engineering: Modern techniques*. London: Springer-Verlag, 2006. 262 p.

8. **Kovalev S.** Testirovaniye elektronnykh ustroystv na proizvodstve: Obzor metodov, analiz dostoinstv i nedostatkov [Testing of electronic devices in production: A review of methods, analysis of advantages and disadvantages]. *Tekhnologii v Elektronnoy Promyshlennosti* [*Technology in the Electronics Industry*], 2013, No. 4, Pp. 66–68. (rus)

9. Electronics Manufacturing Testing – The in Circuit Test & 5 Others. *Versa Electronics*, Feb. 24th, 2020.

10. **Abu Ebayyeh A.M., Mousavi A.** Review and analysis of automatic optical inspection and quality monitoring methods. *IEEE Access*, 2020, Vol. 8, Pp. 183192–183271.

11. **Vaga R.** Industry 4.0 for inspection in the electronics industry. *Proceedings of SMTA International*, Oct. 14-18, 2018, Rosemont, IL, USA.

12. **Rajput P.H.N, Michail Maniatakos M.** JTAG: A multifaceted tool for cyber security. *2019 IEEE 25th International Symposium on On-Line Testing and Robust System Design* (*IOLTS*).

13. **Jamil M.A., Arif M., Abubakar N.S.A., Ahmad A.** Software testing techniques: A literature review. *2016 6th International Conference on Information and Communication Technology for The Muslim World* (*ICT4M*).

14. **Anwar N., Kar S.** Review paper on various software testing techniques & strategies. *Global Journal of Computer Science and Technology*, 2019, Vol. 19, Iss. 2, Version 1.0.

15. **Martynenko N.N., Markova O.M., Rudakova O.S., Sergeyeva N.V.** *Bankovskiye operatsii* [*Bank operations*]. Moscow: Yurayt Publ., 2016. 612 p. (rus)

16. **Thomas S.L., Francillon A.** Backdoors: Definition, deniability and detection. *Proceedings of the 21st International Symposium on Research in Attacks, Intrusions, and Defenses* (*RAID 2018*), Sep. 2018, Heraklion, Crete, Greece.

17. **Ashik M., Jyothish A., Anandaram S., Vinod P., Mercaldo F., Martinelli F., Santone A.** Detection of malicious software by analyzing distinct artifacts using machine learning and deep learning algorithms. *Electronics*, 2021, Vol. 10(14), 1694.

18. **Khorev P.B.** *Metody i sredstva zashchity informatsii v kompyuternykh sistemakh* [*Methods and means of protecting information in computer systems*]. Moscow: Publ. House Academia, 2005. 256 p. (rus)

19. **Kildyushkin R.** Chernyy kod: V protsessorakh Intel nashli dve kriticheskiye uyazvimosti [Black code: Two critical vulnerabilities found in Intel processors]. Izvestiya, 25 march, 2021. Available: *https://iz.ru/1141889/roman-kildiushkin/chernyi-kod-v-protcessorakh-intel-nashli-dve-kriticheskie-uiazvimosti* (Accessed: 16.09.2021). (rus)

20. **Medvedev A.** Put k importonezavisimosti [The path to import independence]. *Sovremennaya elektronika*, 2017, No. 4, Pp. 110–111. (rus)

21. **Erica Portnoy E., Eckersley P.** Intel's management engine is a security hazard, and users need a way to disable it. *EFF*, May 8, 2017.

22. Absolute Software Overview Brochure. 2010 Absolute Software. Available: *https://www.eff.org/ru/node/95854* (Accessed: 16.09.2021).

23. BCM56070 Switch Programming Guide. Broadcom Inc., Aug. 12, 2020. Available: *https://docs.broadcom.com/doc/56070-PG2-PUB* (Accessed: 16.09.2021).

24. **Perevoshchikov V.A.** Complex security systems hardware's vulnerabilities. Aktualnyye voprosy sovremennoy nauki. Sbornik statey III mezhdunarodnoy nauchno-prakticheskoy konferentsii. Dendra, Ufa, 2017, Pp. 5–9. Available: *https://www.elibrary.ru/download/elibrary_29974675_71120736.pdf* (Accessed: 16.09.2021). (rus)

25. Screwed drivers – signed, sealed, delivered. Eclypsium, Inc., 2019. Available: *https://eclypsium.com/wp-content/uploads/2019/08/Screwed-Drivers.pdf* (Accessed: 16.09.2021).

26. **Markov A.S., Tsirlov V.L.** Experience in identifying vulnerabilities in software. *Cybersecurity Issues*, 2013, No. 1(1), Pp. 42–48. (rus)

27. **Begayev A.N., Kashin S.V., Markevich N.A., Marchenko A.A.** *Vyyavleniye uyazvimostey i nedeklarirovannykh vozmozhnostey v programmnom obespechenii* [*Identifying vulnerabilities and undeclared capabilities in software*]. St. Petersburg: University ITMO Publ., 2020. 38 p. (rus)

28. **Zhang B.Y., Yan X.A., Tang D.Q.** Survey on malicious code intelligent detection techniques. *IOP Conf. Series: Journal of Physics*, 1087 (2018) 062026.

29. **Chena C., Cui B., Ma J., Wu R., Guo J., Liu W.** A systematic review of fuzzing techniques. *Computers & Security*, 2018, Vol. 75, Pp. 118–137.

30. **Barabanov A.V., Markov A.S., Fadin A.A., Tsirlov V.L.** Statistics of software vulnerabilities detection during certified testing. *Cybersecurity Issues*, 2017, No. 2 (20), Pp. 2–8. (rus)

31. **Agafin S.S., Smirnov P.V.** Metody obnaruzheniya nedeklarirovannykh vozmozhnostey v programmnom obespechenii vneshnikh apparatnykh moduley [Methods for detecting undeclared capabilities in the software of external hardware modules]. *Bezopasnost Informatsionnykh Tekhnologiy* [*Information Technology Security*], 2014, Vol. 21, No. 2, Pp. 5–10. (rus)

32. **Lipp M., Schwarz M., Gruss D., Prescher T., Haas W., Fogh A., Horn J., Mangard S., Kocher P., Genkin D., Yarom Y., Hamburg M.** Meltdown: Reading kernel memory from user space. *Proceedings of the 27th USENIX Security Symposium*, Aug. 15–17, 2018. Baltimore, MD, USA.

33. **Dorodnov G., Gamayunov D.** Chem opasny protsessornyye uyazvimosti. Chast 2: Spekulyativnyye ataki [Why processor vulnerabilities are dangerous. Part 2: Speculative Attacks]. *Safe-Surf Internet Security Information Portal*. Available: *https://safe-surf.ru/specialists/article/5265/650521/* (Accessed: 16.09.2021). (rus)

34. **Nosov N.** Apparatnoye obespecheniye – istochnik ugroz kiberbezopasnosti [Hardware is the source of cybersecurity threats]. *IKS*, 2019, No. 3, Pp. 89–91. (rus)

THE AUTHORS / СВЕДЕНИЯ ОБ АВТОРАХ

Zelensky Alexandr A.
Зеленский Александр Александрович
E-mail: zelenskyaa@gmail.com

Morozkin Marian S.
Морозкин Марьян Сергеевич
E-mail: m.morozkin@stankin.ru

Panfilov Anton N.
Панфилов Антон Николаевич
E-mail: a.panfilov@stankin.ru

Kuptsov Vladimir R.
Купцов Владимир Романович
E-mail: v.kuptsov@stankin.ru

Gribkov Andrey A.
Грибков Андрей Армович
E-mail: andarmo@yandex.ru

The article was submitted 23.11.2021; approved after reviewing 20.12.2021; accepted for publication 22.12.2021.

Статья поступила в редакцию 23.11.2021; одобрена после рецензирования 20.12.2021; принята к публикации 22.12.2021.