ISSN 0147-6882, Scientific and Technical Information Processing, 2017, Vol. 44, No. 3, pp. 170–174. © Allerton Press, Inc., 2017.
Original Russian Text © V.V. Arutyunov, 2017, published in Nauchno-Tekhnicheskaya Informatsiya, Seriya 1: Organizatsiya i Metodika Informatsionnoi Raboty, 2017, No. 7, pp. 23–27.

On the International Research-to-Practice Conference on Modern Problems and Tasks of Information-Security Assurance (SIB'2017)

V. V. Arutyunov

Russian State University for the Humanities, Moscow, 125993 Russia

e-mail: warut698@yandex.ru

Received April 21, 2017

Abstract—This article considers the results of a conference held at the Moscow University of Finance and Law in April 2017. The conference had three sections: *Information Security Assurance Technologies*, *Data Protection Hardware and Software*, and *Upcoming Trends in Information Security Assurance*. More than 40 reports were presented. A brief review of the plenary and main sectional reports is provided.

Keywords: information security, data protection, information technologies, protective software, information systems, protective hardware, data-protection system, protection efficiency, data-protection indicators

DOI: 10.3103/S0147688217030029

In April 2017 the Moscow University of Finance and Law hosted an international research-to-practice conference on *Modern Problems and Tasks of Information-Security Assurance* featuring more than 150 researchers and specialists. The conference had three sections: *Information Security Assurance Technologies*, *Data Protection Hardware and Software*, *Upcoming Trends in Information Security Assurance*. More than 40 reports were presented.

The conference, which was held for the fifth time, has become one of the country's research & engineering venues featuring people from the scientific and business communities, professors and students, experts, and scientists involved in the field of information security. Its goal is to facilitate efficient communication between developers and consumers of various security products for intensifying the promotion of modern technologies to the market for security tools and systems, as well as encourage the continuation of broad-scale exchange of scientific knowledge among specialists involved in various data-protection fields.

We will present a brief overview of the plenary and main sectional reports that are interesting to Russian and foreign experts in information security.

In his report Peculiarities of Forming Top-Qualified Scientific Staff in the Field of Data Protection in Russia Dr. Sci. (Eng.) V.V. Arutyunov from the Russian State University for the Humanities analyzed Russia's decade-long pattern (2004 to 2013) of training top-qualified scientific human resources (Ph. Ds and Docs. Sci.) in the field of information security and data protection in basic scientific specialties as classified by the Higher Attestation Commission of the Ministry of Education and Science of the Russian Federation. It was noted that considering the demand for information-security specialists, the number of highly qualified scientific staff trained annually in Russia was clearly insufficient not only for the country's Trans-Urals organizations but also for many organizations in the European part of Russia, where they are concentrated in much higher numbers.

According to the data of the report on the citation of theses in scientific literature, which reflects to some extent the interest of one part of the researchers in the results obtained by other researchers and the demand for these results in the scientific community, the fields of significant interest to information-security specialists are personal-data-protection, steganography algorithms and procedures of encapsulating large bodies of data, and information-risk management, including cognitive modeling technologies.

In their report Calculation of Labor Input of Employees Responsible for Information Security of an Organization Dr. Sci. (Eng.) S.B. Veprev and Cand. Sci. (Eng.) S.A. Nesterovich from the Moscow Academy of the Investigation Committee of the Russian Federation considered the average labor input produced by employees of an information and technology unit to maintain CWSs (computerized work stations) in a single-rank and a double-rank system. It was noted that the labor input level is affected by expert knowledge of employees, which is proposed for assessment in a three-chain model and by work experience in information security. The formalization of these parameters is used to propose the procedure for estimating the labor input to make decisions on the quantitative and qualitative structure of employees for the data-protection system.

In their report Advanced Quality Management Standard Technologies Applied in Executing the Training Program for Specialty 10.03.01 Information Security Cand. Sci. (Eng.) N.V. Grishina and G.N. Gudov (MUFL) presented the guidelines for improving the training of students in the specialty *10.03.01 Information Security*. The authors considered present-day management technologies presented in Russian and international standards (corporate management and process management techniques, corporate framework elements and corporate framework design techniques, process analysis techniques, workforce management techniques, information analysis and exchange techniques) and summarized the main sections it would be expedient to add to various courses:

—quality management of electronic tools;

—basic quality-management principles as applied to corporate operations aimed at building a data-protection system;

—elaboration of ideas about quality management as one of the key concepts in the field of management and a means of reaching a required data-protection level;

—formation of abilities to use basic corporate management and process management methods in labor activities;

—digestion of the basics of the modern concept of quality management in development, adoption, and operation of data-protection systems.

In his report System Problems of Personal Data Protection in an Organization Dr. Sci. (Eng.) V.I. Korolev (Institute for Systems Analysis, Federal Research Center Computer Science and Control, Russian Academy of Sciences) analyzed personal data (PD) protection according to regulatory framework requirements. It was noted that the development of a corporate information environment made it necessary to take stock of utilized information resources in all the components of information and technological infrastructure (information systems (IS), engineering information processes, computerized workstations (CWSs), etc.) for determining databases with PD and engineering procedures, where they were utilized. However, to protect the interests of all personal data subjects, it is expedient to set the task of designing informatization/automation object personal data systems as the formation of an integrative system for PD processing and protection in the organization in general.

In their report Typology of Destructive Information Influences in Social Networks Dr. Sci. (Eng.) O.V. Kazarina, E.O. Lisnyak, and M.A. Suvorova (RSUH) provided a classification of destructive information influences (DIIs) according to the typology of the influences and related types of information that is forbidden for dissemination in Russia. According to the authors, the sole method of identifying DIIs in social networks is content analysis with various modifications, including procedures for identification and characteristic appraisal of information found in texts and messages, including electronic messages.

The main areas of research in this field highlighted by the authors are clusterization of social network communities by DII and information forbidden for dissemination; generation of databases of sets of message patterns with text (graphical in the longer view) information of DII; development of efficient algorithms of searching for, comparing, and retrieving information from these databases, and other methods of content analysis of social network information environment.

In their report Information Security Assurance Using Big Data Processing and Data Mining Tools Cand. Sci. (Eng.) P.Yu. Philyak, E.O. Baylarli, V.V. Rastvorova, and V.I. Starchenko (Syktyvkar State University (SSU)) considered various approaches to information-security assurance using information and analysis systems (IASs) that make possible efficient and high-quality analysis aimed at predicting and making management decisions for timely and adequate responses to threats and challenges and based on Big Data Processing and Data Mining.

The practical relevance and efficiency of these approaches are shown based on the example of the Deductor analytical platform, which allows one to build a secure augmentable storage with data in various formats for analysis, and the SAS IAS, and STADIA general-purpose statistical data processing software suite that makes it possible to compute and visualize quantitative parameters of information-security level at protected objects.

In their report Development of a Structure of Indicators for Efficiency Assessment of Information Security Assurance Systems of Information and Telecommunication Technologies at Informatization Objects Dr. Sci. (Eng.) A.N. Fisun from the Oryol State University, Cand. Sci. (Law) Yu.A. Belyavskii from the Central Russian Institute of Management at RANEPA, and R.A. Fisun from the Smolensk Oblast Unit of the Main Branch of the Bank of Russia in the Central Federal District analyzed the procedure for forming a structure of indicators for efficiency assessment of tools and systems of integrated information-security assurance of information and telecommunication technologies (ITCTs), including information systems (ISs), information and telecommunication networks (ITCNs), of informatization objects of public authorities, agencies, organizations, establishments, enterprises that operate under risk, uncertainty, and artificial and natural internal and external threats: they are characterized by a large diversity of quantitative and qualitative efficiency criteria and indicators. This procedure is implemented in five phases.

In the first phase, a set of indicators is formed that characterize the quality of the developed or upgraded system and Integrated Information Security Assur-

ance Tools (IISATs). These indicators make efficiency comparison of these IISATs with basic examples possible. In the second phase standardized and reference requirements on (criteria for) IISATs are justified or selected. In the third phase the integrated system of quality indicators (ISQI) of IISATs is standardized. In the fourth phase the efficiency of the developed version is estimated. In the fifth phase conclusions are formulated about the engineering and economic efficiency of the product and recommendations given on upgrading and adopting the proposed version of data-protection system and control system tools.

In his report Social Aspects of Information Systems Development Dr. Phil. I.N. Belogruda from the Financial University under the Government of the Russian Federation presented the data collected by Russian Public Opinion Research Center during Internet user surveys. While 53% of the respondents answered that the Internet has a positive impact on their lives, 27% of those polled considered it a threat to family values and political stability, and approximately 20% said that they have faced problems of data security in social networks. The most typical data-security problems are password theft (26%) and account hacking (~70%). Moreover, according to slightly more than 23% of the those polled, the intruders claimed to be the actual users and tried to obtain money from their friends. According to other data from the report, active users of information technologies face the problem of perceptive changes. Moreover, the users who spend a large amount of time in their social network accounts online are more frequently susceptible to stress. First of all, this phenomenon is typical of users who do not present their real image but try to create an alternative version of their personality.

In their report Efficiency Assessment of Information and Communication Systems Immunity Cand. Sci. (Eng.) A.G. Korepanov, I.S. Trubin, and Dr. Sci. (Eng.) I.A. Chastikov from the Vyatka State University (VSU) analyzed various approaches to efficiency assessment of the immunity of information systems. The approach proposed for use in teaching and learning activities is based on statutory instruments that are in effect and the Delphi procedure.

A training program for assessment of the efficiency of information and communication system immunity has been designed at VSU. Its implementation is based on using regulatory instruments in effect and the Delphi procedure. The result of the program is the evaluation of the immunity of a studied information system. The output of the program operation results in a special file is meant for the subsequent processing of the data.

In their report System Dynamic Modeling Procedures Applied to Solving Information-Security Assurance Problems Dr. Sci. (Eng.) V.A. Minaeva, E.V. Waits, Yu.V. Gracheva, N.A. Shalny, and A.A. Storozheva from Bauman Moscow State Technical University considered the main research areas of simulation modeling of information-security systems, with particular focus on analyzing system dynamic models of information-security systems. The results of this analysis showed that this problem area has been actively investigated by foreign research teams. Moreover, the system dynamics approach offers very promising opportunities and the attained modeling results are of particular research and practical interest. It is possible that future system dynamic models of IS systems will be designed and studied at both a high level of aggregation (when solving general concept problems) and a detailed level (when specific practical aspects of IS systems are considered). All available system dynamic models of IS systems include a relatively limited number of factors, the range of which calls for further studies.

In their report Recruitment of Employees for Corporate Competitive Intelligence I.A. Rusetskaya (RSUH) and A.V. Tumanova (Podmoskov'e Agency of Information Systems) noted that competitive intelligence specialists are usually divided in two groups, i.e., former security-service employees and marketing-science analysts. The report considers the principles of and approaches to recruiting competitive intelligence specialists in the light of the requirements of enterprise information-security assurance.

In addition, the statistics about the reasons for selecting employees for the competitive intelligence unit were presented. In particular, when they hired an external specialist for work in the competitive intelligence unit, 75% of the CEOs chose former employees of law enforcement or defense and security agencies, whereas 60% opted for in-house employees, not outsiders.

It was concluded by the authors that marketing-science analysts and security specialists are in nearly equal demand in Russia; however, the latter are given an unspoken priority during hiring in the competitive intelligence unit. Most CEOs were confident that information-security specialists would be more reliable and had better knowledge of this field of activity. However, according to statistics from companies in the West, competitive intelligence units are dominated by marketing-science analysts.

In her report Information Transfer Network Modeling Software G.M. Antonova from the Trapeznikov Institute of Control Sciences of the Russian Academy of Sciences considered packet network simulators that are suitable for developing simulation models of computer networks while checking the quality of designed information-security tools.

The report considers the NS-2 packet network simulator, which helps to solve various abnormal traffic research problems and form evaluations of network characteristics, the NS-3 simulator, which allows modeling computer networks at various engagement levels, i.e., WWW, Mobile Networking, Satellite Networking, LAN, etc., and the Cisco Packet Tracer and

NetSim simulators, which were designed for computer networks based on Cisco products. The author highlighted the need to develop an upgraded technology of building computer models of the data-transfer network and organizing model timers, simulating routing procedures, serial connection of protocols of various levels, and replacement of protocols while studying the network model.

In their report Studying the Impact of DOS Routing Attacks on Operating Behavior of Wireless Sensor Networks E.Yu. Golubnichaya and D.A. Repechko from Volga State University of Telecommunications and Informatics considered the results of simulation modeling of a wireless sensor network with one of its nodes showing malicious behavior. The modeling environment was the open-source code Network Simulator 2.

As noted by the authors, information-security assurance is especially important to intensively developing wireless sensor networks (WSNs). The high level of impact of various types of logical DoS routing attacks on the operating behavior of WSNs is confirmed by the results of simulation modeling. It was stated that even a small number of nontransferred information packets (e.g., data packets with information on an outbreak of fire on a certain territory controlled by the sensor) can cause catastrophic situations in many WSNs. Considering the increased susceptibility of WSNs to various kinds of attacks, the authors considered it necessary to utilize not only traditional means of information-security assurance (authentication cryptography, etc.) but additional means of intrusion detection as well.

In their report Comparative Analysis of Instrumental Programming Languages for Information-Security Assurance Problems Cand. Sci. (Eng.) A.D. Kozlov and Cand. Sci. (Ped.) M.S. Shapovalova (RSUH) compared a number of modern programming languages for the purpose of their efficient selection to solve information-security assurance problems. The languages are Python, Perl, C++, and JAVA. According to the information (as of June 2016) given by the authors about the TIOBE index used to measure the popularity growth of programming languages, JAVA has the first spot among TOP-20 languages, with a large gap between C, which is in the second place.

The authors compared the programming languages according to program code relocatability, hardware minimization, and the processing speed of programs. According to the analysis, the authors concluded that the combination of C++ and JAVA is the most efficient means of program design for information-security assurance.

In her report Cognitive Biases As Information Security Threats and Procedures of Their Rejection Cand. Sci. (Eng.) A.A. Kononova from the Institute for Systems Analysis, Federal Research Center Computer Science and Control, Russian Academy of Sciences, considered the threat of cognitive bias generated by consistent deficiencies in informing about existing problems of information-security assurance. Essentially, this bias is the cause of most accidents, emergencies, and catastrophes, which is commonly referred to as the human factor. The author proposes viewing cognitive bias as an information-security threat. In addition, criteria-modeling procedures are proposed as the means of their rejection.

The most basic version of criteria-modeling techniques was adopted in a series of Bank of Russia standards of maintenance of information security of the Russian banking system organizations (STO BR IBBS). These procedures have a more complex form in the Vanguard software suite for managing the security of e-payment technologies in the regional settlement systems of the Bank of Russia and a whole range of critical infrastructural facilities. In conclusion, the author noted that criteria-security modeling procedures are currently being developed in parallel with instrumental techniques for information-security assurance.

In their report Modeling the Dynamics of Information Security Threats Dr. Sci. (Eng.) V.A. Minaevam E.V. Waits, and Yu.V. Gracheva from Bauman Moscow State Technical University considered building a dynamics model of eight organization-relevant information-security threats and the implementation of this model in Anylogic simulation software. A hierarchical system dynamic model of information-security threats was proposed and implemented in the same software. The bottom level in the hierarchy is occupied by system dynamic models of processes for separately countering each particular information-security threat. The dynamic curves of risk levels of information-security threats, a diagram of accumulating dynamics, and dynamic curves of sets of threats with acceptable and unacceptable risk levels were derived. The model and experiment make it possible to track the dynamics of sets of threats against the risk level dynamics of each particular information-security threat.

In their report Analysis of Means and Procedures of Traffic Interception in DLP Systems Cand. Sci. (Eng.) A.V. Kryzhanovskii and I.G. Generalova from the Volga State University of Telecommunications and Informatics justified the expediency of utilizing the DLP technology for building a secure corporate network to prevent confidential information leaks from an information system. It was noted that information in DLP systems is recognized mainly by the linguistic and the statistical techniques.

A comparative analysis of Russian and foreign DLP products was conducted; its results were used to justify the choice of the DLP product for building a secure corporate network. The considered and studied techniques of information-leak prevention that are used in the given systems include:

—network interception based on the ability of several controllable network switches to duplicate network traffic from one or several ports to some other port;

—agent interception based on agent application used as programs or services to intercept traffic from network workstations;

—several other techniques.

In addition, the possibilities of integrating various DLP systems are considered.

The collected papers of the conference participants published by the MUFL by the beginning of its work *Sovremennye problemy i zadachi obespecheniya informatsionnoy bezopasnosti: sbornik statey Mezdunarodnoy nauchno-prakticheskoy konferentsii SIB-2017* (Modern Problems and Tasks of Information Security Assurance: Coll. Papers of Int. Research-to-Practice Conf. SIB'2017), Moscow, 2017, 220 p.) are included in the publications processed in the Russian Science Citation Index (RSCI).

Translated by S. Kuznetsov