software are offered; the verification technique software on existence of destructive properties for environments of cloud computing is synthesized.

As development tendencies of the ISIS use are the following [1, 4]:

– improvement of system architecture of IS in CIS providing effective management in the conditions of uncertainty of a condition of the information environment;

– development of new models of counteraction to threats of violation of IS in CIS on the basis of a choice of optimum option of response to safety events;

– improvement of tool program complexes with intellectual support of decision-making with research of efficiency of methods, models and algorithms;

– development of technologies the multi-agent systems for detection of attacks, counteraction to threats of violation of IS, an assessment of level of security of information in CIS.

**References**

1. *Mashkina I.V.* // Control systems and information technologies. Voronezh, 2008. No 2 (32). P. 98–104 pp.

2. *Rahimov E.A.* Models and methods of support of decision-making in intellectual system of information security. Abstract PhD on speciality 05.13.19. Ufa: UAI, 2006.

3. *Tumanov Yu.M.* Protection of environments of cloud computing by software verification on existence of destructive properties. Abstract PhD on speciality 05.13.19. M.: MIFI, 2009.

4. *Vishnyakov V.A.* // Proc. of 4th Int. Conf. OSTIS-2014. Minsk: BSUIR, 2014. P. 373–376.

## INFORMATION SECURITY TOOLS AND THE USE OF INTELLECTUAL AGENTS

ZAHRA GHNABARI, V.A. VISHNYAKOV

The analysis of methods and means of information protection in information systems is done. The directions of intellectual systems in data protection (ISDP) are given. Learn about how to use expert systems, neural networks, and their combination in DP. The promising method explains how to use intellectual agents in ISDP.

The methods of information protection include: management, obstacle, regulation, motivation, compulsion, concealment of information. Information security tools include: formal (technical, software), informal (organizational, legal, moral and ethical). Levels of information protection can be: the hardware and software, procedural, administrative. legislative. The protection system components: physical security, safety personal, legal security, safety equipment, security software, security is telecommunication environment. Organizational protection measures determine the order: reference system of protection from unauthorized access; restrict access to premises; assignment of access; control and accounting of events; software maintenance; control of protection system.

Implementation of the system of information protection passes steps: the solution concept, system design, implementation, maintenance, sanctions. This are: engineering survey and description of information resources system; identifying the most critical places of the system; probabilistic assessment of threats to the security of information resources; economic evaluation of damage; value analysis of possible ways and means of information security; define profitability of information security systems.

It is must be protected from the point of software view: against loss (backup), invalid access (encrypt, restrict), invalid modification (electronic signature).

Along with the traditional means of protecting enterprise systems: antivirus, detection of vulnerabilities, firewalls and intrusion detectors. The applied automation tools are used including event correlate's, program updates, authentication, authorization, and administration, risk management systems.

Intellectual systems of information protection (ISIP) are devoted the attack detection systems. As a predictive tool ISIP use neural network (NN), the system of fuzzy logic and expert systems (ES). The scheme of attack detection includes detecting abuses and anomalies [1]. In ISPI the knowledge base of ES contains the descriptions of the classification rules according relevant user profiles and the scenarios of attack on the information system (IS). Disadvantages of ISIP on ES: system is not adaptive, its not detect always unknown attacks [1].

If NN is represented as a separate attack detection system, the analysis information for abuse during traffic processing is realized. The cases to attack are directed to security administrator. Approach is speed, since only one level of analysis is used. One of the disadvantages of the NN is the opacity of the analytical results.

The next type of detection systems includes the use of NN supplemented by ES. The sensitivity of this system increases, so the ES gets the data only about the events which were regarded as suspicious. If the NN at the expense of the training was to identify new attacks, the knowledge base of ES should be updated [1].

The use of hybrid neuro-expert systems or neuro-fuzzy systems let to reflect in the system structure the fuzzy predicate rules which are automatically adjusted during NN training. The adaptive fuzzy NN let to solve individual tasks to identify threats comparing the behavior of users with existing template system and automatically configure new rules when changing field of threats [1]. A new trend in ISPI is the use of intellectual agents (IA) working in a distributed IS and programmed for search as the invasion and anomalies [2]. The following areas of IA use in information protection are identified: research on attack detection systems (ADS); automation of search in IP (organizations, technologies, services, etc.); intellectualization of decision in DP [2].

The use of multi-agent systems for IP is discussed in work [2]. In this case it is necessary to investigate widespread attacks on the information system and the process of implementation of the attacks; investigate the existing systems of attack detection and attack detection methods; design a multi-agent structure and composition of the ADS. Its develop the structure of agent in attack detection system; work out the model for knowledge representation of agents about the state of information system; develop the method of joint analysis by agents of the information system state. The multi-agent architecture ADS involves many interacting intelligent agents. The standard IS components, sources of information to be analyzed for attack detection are proposed. The structure of agents, which includes modules: management, receiving and processing data, analysis, training, response, generate messages, making a decision. The function of modules are describes. Methods of work with a multi-agent ADS includes steps; placement agents by blocks of IS; data collection, the formation of training set, attack detection, and reporting it to the administrator.

**References**

1. *Kalach A.V., Nemptina E.S.* // Internet magazine «Technology tehnosfera security» (http://ipb.mos.ru/ttb). № 3. 2011. P. 3–11.

2. *Nikishova A.V.* Izvestia JuFU. Technical science. Theme issue. «Information security» — Taganrog: TTU, JuFU. 2012. № 12 (137). P. 28–33.

## ОБЗОР И АНАЛИЗ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В ЭЛЕКТРОННОЙ КОММЕРЦИИ

В.А.ВИШНЯКОВ, ХРАЙБА МОХАММЕД

В докладе представлены результаты анализа применения средств защиты информации в электронной коммерции (ЭК). Выделены следующие направления: угрозы и технологии их предотвращения, действия по защите в ЭК, услуги защиты для ЭК, две технологии шифрования (симметричная и асимметричная), использование