# СЕКЦИЯ 3. ЗАЩИТА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ И ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

## SCADA SYSTEMS SECURITY

Al-Kamil Iehab Abduljabbar Kamil, N. Nasonova

Supervisory Control and Data Acquisition (SCADA) system is aimed at automatic controlling or monitoring the data and is composed of number of remote terminal units (RTUs) for collecting field data, hosts and nodes. SCADA systems cover large geographic areas and often require the use of wireless communications, supporting TCP/IP, UDP or other IP-based communications protocols as well as strictly industrial protocols. SCADA systems are exposed to the same cyberspace threats as any business system because they share the common vulnerabilities with the traditional Information Technology systems. Among the requirements to the SCADA systems security the following are suggested:

– critical components protection from cyber attacks, failures and strong safety policies and procedures development;

– knowledge management and training competencies for the personnel, based on policy, standards, design and attack patterns, threat models, code samples, reference architecture, and secure development framework;

– SCADA systems development, considering system security development starting from early stages and during the whole software development cycle, implementing the secure software development principles; this also concerns the security issues implementation in the devices;

– vulnerability analysis based on proactive, discovery, and adaptation solutions;

– the basic mechanisms to ensure network security for SCADA systems include authentication, confidentiality, integrity, availability, and nonrepudiation.

## USE OF INTELLECTUAL AGENTS FOR INFORMATION SECURITY OF CORPORATE INFORMATION SYSTEMS

U.A. Visniakou, M.G. Mosduany Shiras

The methods of information protection include: management, regulation, motivation, compulsion, concealment of information. Information security tools include: formal (technical, software), informal (organizational, legal, moral and ethical) methods. Levels of information protection can be: the hardware and software, procedural, administrative. legislative. The protection system components are: 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.

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. 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.

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 neuron net (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. 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. 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.

The use of multi-agent systems for IP is following. 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