***Bashynska Iryna**, Odessa national polytechnic university,*
PhD in Economic Sciences, the Department of Accounting, Analysis and Audit

Ensuring economic security of modern enterprise as a systematic approach

Abstract: This article is devoted to modern means of protection the economic security of enterprise. The publication focuses on the differences and advantages of different means of ensuring economic security which mainly provide protection from physical penetration.

Keywords: economic security, security system, enterprise, alarm system, video surveillance systems, access control system, intelligent video analysis, biometric access control system, inspection scanning equipment, perimeter protection systems.

In an area of rapid technological globalization of labor, capital, and product markets, old economic notions of a trade-off between "efficiency" and "equality" have been replaced by a more nuanced understanding of the interdependence of economic and social development [1]. Nowadays the information sector is leading in the state and have an impact on all elements of the functioning of the enterprises. Together with the increasing dependence on electronic technology related to the spread of information and growing threat of cyber-attacks, the aim of which usually become information resources and network infrastructure. Evaluation of the safety management system of industrial facilities in Ukraine has found the urgent need of drawing a current mechanism of software and hardware that is designed to develop and implement management actions on technological object. Industrial activity requires personal attention to ensure the safety of its facilities, personnel and intellectual property. This raises the issue of enhancing the security of digital networks and infrastructures particularly relevant.

Under the economic security, understand the economic system, which is characterized by the presence of competitive advantages, which are achieved by efficient use of existing own and borrowed resources, timely introduction of a set of measures to maintain normal system performance to maximize the achievement of objectives in the short and long run in constant changes in the environment [2].

Based on the tasks facing the service of economic security to provide the information and analytical security, consider the means complex security system based on advanced information technologies and the equipment of leading world producers.

1. *Alarm system* (AS) intended for the detection the unauthorized access to the protected object and respond to penetration.

AS consists of the security panel, which collects and analyzes information of alarm sensors, and performs programmed therein it functions when sensors operated. Dashboard displays the status of the alarm, is used for its programming, setting and removing the object of protection. The most common security sensors – three-dimensional infrared, acoustic, vibration, ultrasound, radiation, capacitance. With AS also possible to monitor the power supply, temperature, gas leaks, water leaks, etc. Burglar alarm systems are divided into: wired, wireless radio alarm. They also divided by type of signaling: hot (sounds siren) and console (signal goes to the fixed post security).

2. *Video surveillance systems* (IP-CCTV) intended for the organization of video on the objects, they can also be used: as counter actors (individuals, vehicles), for the analysis of certain events, as standard safety video surveillance to capture evidence of theft, etc.

IP-CCTV use in data transmission encryption and authorization system for complete privacy. Control and administration of the system is of any computer that has access to the network and special software. IP-CCTV integrates with fire alarm systems, security alarm systems, access control, as well as any modern mobile device.

3. *Access control system* (ACS) allows to fix and process the information about each item passes through the restriction of access, and protect the premises from unauthorized access, regulate access. As a subject can act as individuals and vehicles.

As the subject identifier used the physical medium (key-"tablet", contactless card, key chain), and codes that are entered from the keyboard, also to identify a person used signs his biometric (fingerprint, iris photography).

For security organization while entering the territory that may be imposed antiramming bollards. They are the most reliable blocker and often belong to a class of anti-terrorist barriers.

Network access control managed by a central computer and can create reports on the events: the passage of the territory of employees, keep records and control subjects according to the set parameters.

4. *Intelligent video analysis system* (IVAS) provides an advanced solution that performs intelligent video analysis and fully automates video monitoring. It automatically tracks and identifies objects, analyzes motion and extracts video intelligence from analog, digital, or IP video streams. These analytics can output real-time events and object data for video data mining or storage in a database. IVAS integrated with CCTV and makes it possible to:

- object recognition (people, car numbers, posted items, providing a potential threat and other factors);
- registration violations manner.
- integration with databases of photographs, license plates to identify terrorists, criminals, delinquents.

With this system, power structure can solve the problem of security on qualitatively new level, always respond promptly and take appropriate action.

5. *Biometric access control system*. In especially important areas of law enforcement agencies is recommended to use an access control system with biometric identification technology, which allow recognizing the human personality with high efficiency by:

- the fingerprint;
- the image of the person;
- the iris of the eye.

Biometric access control system allows you to:

- effectively distinguish between employees and visitors access to area departments;
- significantly reduce the risk of leakage of confidential information theft and unauthorized access.

Physical access control biometrics includes everything that requires identity authentication by scanning a person's unique physical characteristics. It is used where high security is a necessity due to its superiority compared with conventional access control methods. Hospitals, police, the military as well as the financial industry all use physical access biometrics for the purpose of greater security and efficiency.

The New Generation of Smart Devices in Biometrics for Access Control enhances building security, internal communications, and employee management, at a significantly lower total cost of ownership than previous biometric systems for physical access control. Whether being used to access a building, secure restricted location within, or for time and attendance management, biometric authentication technology has come a long way. Just a few years ago, the debate surrounding biometrics was focused on whether biometrics were accurate and could handle large populations, among many other operational issues. Today, these arguments are closed: the focus now is on enhancing the value associated with accurate and secure biometric authentication.

Today, biometric security devices do much more than authentication: they also provide the right level of security, at the exact places needed, and are able to adjust dynamically the level of authentication necessary for ever-changing threat levels. These capabilities only increase in importance as modern physical access control systems also begin to converge with other building management and communication devices. To manage employees, visitors, and contractors better, and protect important areas – executive floors, data centers, and research labs – more companies are deploying physical security systems, video surveillance cameras, and time and attendance systems.

The security services is successfully used biometric technology in combating terrorism and transnational organized crime, drug trafficking, illegal migration, modern forms of slave trade, organization of public access to the premises where it is stored, processed and circulated classified information, and more.

6. *Inspection scanning equipment*. Items of particular importance must be equipped by scanning equipment. This equipment can detect the materials and items used for terrorist attacks, for inspection of mails and hand luggage to detect explosives, drugs and toxic substances.

Metal Detector – is one of the most common types of Inspection Equipment, which are basically of two types: manual (for a review of a particular baggage) and arched.

Hand-held metal detectors are compact, easy to handle. Through them, you can quickly check any man, his hand baggage for the presence of metal objects (including firearms and bladed weapons, any metal parts).

Arched stationary metal detectors are usually used to control and verify the number of people (up to 3000 people per hour). Depending on the design, arched metal detectors are single-band and multi-zone.

The latest mean of ensuring economic security is 3D scanning on CMM – a powerful combination delivering high inspection accuracy and throughput. A CMM equipped with a laser scanner boosts 3D inspection processes. CMM laser scanners simplify preparation of inspection jobs, excel in measuring speed and capture the entire geometry of part surfaces and features with metrology accuracy. Different scanner types are available, providing choice options related to accuracy, laser stripe, standoff distance and field of view.

7. *Perimeter protection systems*. Perimeter protection system control the outer perimeter of the object, which is the first and most important border protection and any unauthorized penetration should cause alarm indicating the exact location of the invasion.

Perimeter security systems included in the overall system security alarm and is based on radio wave or capacitive sensors, vibration-sensitive sensors with sensor cable and / or wiretension systems for perimeter protection. The range of possible remedies perimeter area is large enough and each enterprise selects the most appropriate for their needs. The most common are:

- Fence Detection Systems – next-generation fence-mounted sensors that detect cut or climb attempts and pinpoint intrusion attempts to within 3m / 10ft.;
- Buried Cable Detection Systems – terrain-following volumetric sensors that locate intruders to within 3m / 10ft for applications where covert protection is essential);
- Alarm Monitoring – advanced security management systems that monitor, display and control a facility's complete perimeter security program;
- Microwave Sensors – short or long range volumetric microwave links and transceivers for open areas, gates, entryways, rooftop and wall applications;
- Relocatable Microwave Sensors – rapid deployment microwave links and transceivers for the protection of VIPs, mobile assets or other temporary high security applications;
- Infrared Sensors – advanced, stand-alone high-performance sensors for short and medium range outdoor intrusion detection applications;
- Dual Technology Sensors – outdoor dual technology motion sensors offer the unique combination of Doppler Microwave and Passive Infrared technology.

Thus, of the above means of protection the informational component of economic security of enterprise selects those that solve the necessary tasks the best way. An enterprise may use separate means or integrate them, thereby achieving the synergistic effect and increasing their overall efficiency. With insufficient budget most efficiently will provide a minimum protection "from all sides", i.e. choose the cheapest means. Later, after testing the existing system, the enterprise can provide additional protection "bottlenecks" or strengthen information protection for those areas of the enterprise, which are most often exposed to malicious attacks.

References:

1. Plotnick R.D., Meyers M. K., Romich J., Smithold S. R. Assumptions, New Realities. Ensuring Economic Security for Working Families in the 21st Century. London, 2013. - P.272
2. Башинська І.О. Розділ 3.2. Уточнення визначення дефініції та економічного змісту категорії «економічна безпека підприємства» (С. 14-20) у кол. монографії Економічна безпека в умовах глобалізації світової економіки: [колективна монографія у 2т.]. – Дніпропетровськ: «ФОП Дробязко С.І.», 2014. – Т. 2. – 349 с.