STOCHASTIC SYSTEMS. SECURITY PROVISIONS

The development and intellectualization of the logical level of processing, the adoption of the Radio Frequency Identification (**RFID**) technologies, the establishment of the Internet and origination of its varieties – **The Internet of Things, Medical and Expanded Internet**, the massed advance to the assimilation of the physical level of processing started by them as well as stipulated their deep system transformation with an entry to the nano-level of processing is a complex and internally contradictive process.

On the one hand it leads to deep qualitative reorganization of economic and social relations and on the other hand, – to the increase and drastic aggravation of security threats.

The problems for provisioning security acquire the increasing, especially important role, which is caused by the following factors:

- Unprecedented increase in the production and distribution of adulterated products, the increase in the sales of poor-quality and uncertified products, increase in the number of thefts, burglaries and car theft,
- The continuing globalization of the information space and transfer of key functions of control and management to automatic and robotic systems,
- The ongoing attempts to attain one-sided advantages by means of the technological pressure, real and latent cybernetic threats, introduction of undercover beetles, unfair competition and propaganda of defective solutions of inferior quality,
- The anticipatory growth of technological availability of criminals,
- The expansion of the scales and possible directions for performing destructive attacks.

It has become possible to solve high-profitably and efficiently the key problems in the field of security provisions at a qualitatively new and efficacious level due to the pioneering works of Auto-ID Labs, the development of the EPCglobal concept, the achievements in radio engineering and microelectronics (Hitachi, NXP Semiconductors), in system analysis and a breakthrough based on the discoveries in the field of algebra (I. A. Kulakov, 2005, 2010), the development of a new innovative direction – ***stochastic technologies***.

With the introducing and hiding the private keys, not otherwise, ***stochastic technologies, as well as products (hardware, software) being made on their basis pass into cryptographic ones***. Stochastic technologies cover all topics of the modern symmetric cryptography; they are aimed at the perspective and open up new possibilities in the field of theory of systems, statistical modeling and security provisions. *They have an overwhelming superiority in all the characteristics over the existing analogues* [1].

The efficacious, profitably and energy efficient protection of system elements from cloning and counterfeiting based on stochastic technologies (RFID/EPC tags and microsensors, silicon and organic, in fact not leading to the increase in their cost price and power consumption) will make it possible to solve sequentially the following applied problems within a short time by using the existing technological basis:

1. Protection of goods and products from adulteration and counterfeiting, distribution of solutions to the tasks of money payments, remote payment of services, access regulation and access control, protection of certifying documents and currency, marking of the post, archival documents, exhibits and the library stocks, identification of domestic animals, etc.
2. Implementation of highly cost-effective protection of composite and complex objects (from simple packages and their elements to assemblies and their units and parts) by integrating electronic protection with low-cost production and technological means from simple numbered labels to laser engraving, distribution of the technologies to the economy sector (pharmaceutics, transport, etc.).
3. Transition of the control system for the goods quality and monitoring of the environmental state as well as systems providing ecological, biological, physical and engineering and technical security to a qualitatively new level by equipping tags and microsensors with multifunctional sensitive mini-transducers, which are based on smart materials produced by the modern bio- and nano-industries.
4. Production upon mastering of noise-immune multichannel wideband and acoustical radio-frequency technologies of protection systems of vitally important objects, dwellings and buildings,

protection of distributed engineering and technical infrastructures from unauthorized actions under conditions of industrial and intentional electromagnetic noises.

5. System integration with advanced high-level solutions of such business organization as SAP and HP, the mastering of new generation technologies developing together with adaptive technologies of integration of system elements such as smart buildings, community facilities and complexes, smart dwellings (smart houses), landings and housing cooperatives.

One of the key moments of solutions is the introduction of a highly efficient (the performance being tens of billions of keys per second), centralized system of key management, as well as the provision of all categories of customers with authorized and individual devices for authentication of products and goods and their quality check, namely

- low-cost pocket and mobile autonomous devices of direct control as well as local and high-level network plug-in units and add-in devices, in particular, for computers and telephones.

Setting up large-scale production of the above-mentioned devices, it becomes possible ***to attract different groups of population to organization of the total protection of segments of national and world goods market and economy from illegal and poor-quality products***. In this respect, the example of the rushing development, assimilation and return of mobile **NFC** (**Near Field Communication**, Nokia) technologies is illustrative.

As one can see in the perspective, upon development and thorough approbation of stochastic technologies, it will become possible ***to create highly efficient standard cryptographic primitives and parallel cryptographic co-processors***, aimed at information processing per terabit per second. Their mastering will allow one, without a visible decrease in the performance of computer, information and communication, TV and satellite systems, communication facilities, positioning and navigation, to solve on a qualitatively new level the problems of

- information security, prevention of massaged cybernetic attacks, real and latent cybernetic threats, unauthorized access and unregulated action, protection of copyrights, in particular of audio and video products, programs and literature.

In addition, stochastic technologies allow simple and efficient realization of the **Phisical Unclonable Function** (**PUF**), implemented in the physical structure of microchips by means of random delay variations in semiconductors and transistor shutters. These functions can be used to realize

- non-linear, high-quality generators of true random numbers and probabilistic cryptographic authentication protocols, unlike the known approaches, with the assured and proved reliable statistics and cryptographic resistance, as well as embedded protection of microchip memory from direct penetration, etc.

The above-mentioned problems can be solved based on the Concept of Security Provisions, proceeding from the development of information and wireless technologies, microsensor (**RFID**) and cyber-network technologies, worked out by the leading Russian scientists and engineers, strengthened by the newest fundamental research, world experience and applied scientific and technical developments.

In order to apply in practice the scientific and technical achievements mentioned in the Concept and to eliminate the drawbacks, which result in a considerable slowdown of distribution and development of electronic systems, **it is proposed to combine the efforts** for modernizing the EPCglobal system and integration with high-level applications of business organization, to transfer **RFID** technologies (radio-frequency tags of EPC, UCODE and I-CODE, µ-Chip), as well as microsensor technologies, technologies of production of smart-materials and technologies for security provisions on the whole, as is predicted by the experts, to the level compared to the revolutionary one.

In this extended substantiation, ***the presented technologies, with respect to scales, returns and significance, become comparable with a highly-developed economic segment*** and with respect to importance, they pass to the national and interstate level, thus making it possible *to take the leading part in the world* in the field of security provisions, the development of cryptography, bio- and nano-industry, electronic and information-communication systems.

Looking into the future, with the development of the production of sensitive (smart) materials and the element base endowed with intellectual functions and of the technologies of their adaptive network integration, ***microsensor technologies are inevitably replacing the RFID technologies, and after them – local and global cyber-networks***, which are constructed on the basis of noise-immune ultra-

wideband (**UWB**) and wireless (**NFC**, **Bluetooth**, **Wi-Fi**, **ZigBee**) technologies, surface (**GSM**, **CDMA**) and satellite (**GLONASS**, **GPS**, **Galileo**, **Běidǒu**) systems.

As research and forecasts show, cyber-networks will cover and naturally conquer the world – from monitoring systems of the environment, homes, purses and currency to technological systems, production complexes, medical institutions and land – and will penetrate to deeper material levels. Under conditions of potentially dangerous and real cybernetic threats, introduced by them, non-eliminated great-power ambitions in the interconnected world, destruction and pollution of the habitat of living organisms, as well as an increase in the scales of distribution of products dangerous to the human health, the growth of terrorism and high technological availability of criminals, the ***solutions laying the foundations of the Concept presented in the Appendix will also become a reliable help and efficacious tool for providing the State security of countries and their citizens***.

Appendixes – «**Innovation Breakthrough in the Field of Microsensor** (**RFID**) **and Cyber-network Technologies**» and «**Concept of Security Provisions**» are presented separately.

With a view to a long-term prospect, by retaining the succession of the developments while moving from simple to more complex, **as the first step for realizing** the above-mentioned Concept, participation is suggested in a short-term parity project – «**Substantiation of Realization of a Minimalistic Authentication Protocol of Low-cost Identification Radio-Frequency Tags**», which involves insubstantial investments and is characterized by high returns in comparison with analogous developments being realized at present.

Aim of the project. Substantiation of realization of efficacious, highly profitable (without increasing the cost price of production) and energy efficient (without decreasing the radius of action) embedded electronic protection from cloning, imitation (emulation) and counterfeiting of low-cost silicon and organic, non-rewrite (**RO** type) identification radio-frequency tags (**ID** RF-tags).

Due to the introduced solutions, the hardware realization of the radiofrequency interface and one-side authentication Protocol is characterized by low energy consumption, linear and simple topology and a very small number of logical elements (30 triggers and 300 transistors – 75 **GE** per kernel of the one-side function, 2 triggers and 40 transistors – 10 **GE** for adding complexity to the design), with the 71-bit length of the private key embedded into the microchip and the cryptographic resistance of no less than 2^{57} achieved within 16-17 rounds (serial one-bit polls), which, according to the criteria of time and financial expenditures necessary to crack protection, is sufficient, at least for the next decade, for the planned applications on based low-cost **ID** RF-tags. In realizing mutual, two-side authentication Protocols, the number of logical elements increases insignificantly – by 3 triggers and 14-16 **GE** – with the kernel remaining the same, exceptionally due to changes in the complexity function.

As a result, the total hardware expenditures required to realize the authentication Protocols constructed on the basis of the stochastic technologies are in the order of 150-200 **GE**, which is 15-20 times less that in the counterparts constructed on the basis of the most known cryptographic primitives (**AES-128**/3400 **GE**, **TEA**/2633 **GE**, **Trivium**/3091 **GE**, **Grain**/3360 **GE**). In addition, the proposed ***light-weight cryptographic primitives***, which require for their realization about 1000 **GE** and a large number of rounds, as well as widely spread, low-cost primitives (such as **A3**/**A5** and **Crypto-1**) used in the **GSM** systems and contactless **Mifare Classic cards**, but discredited with respect to technical and cryptographic indices, cannot offer any serious competition.

Potential consumers of the results are the leading Russian and Foreign manufacturers of **RFID** tags (**Angstrem**, **Sitronics**, as well as **Hitachi**, **NXP Semiconductors**, **PolyIC**) and large system integrators (**Systematica**, **RusNano**, as well as **EPCglobal**, **Symbol**, **IBM**, **HP**, **Philips**, **Siemens**, **Nokia**, **SAP**, **Microsoft**) etc.

---

[1] Development of stochastic technologies leads to the improvement of the methodological basis, assumes the development, unification, and standardization of the mathematical methods and approaches of the cryptographic analysis of applied applications based on them. In turn, this will allow one to achieve the optimal combination of the cryptographic resistance and design of software and hardware solutions as well as to decrease substantially high costs on expertise, certification, and licensing of commercial products.