Principles of information security management system

V Y Dronov and G A Dronova
Novosibirsk State Technical University, Novosibirsk, Russia

E-mail: dronov@corp.nstu.ru

Abstract. The main element of a complex system that determines its performance and efficiency is its management system. Modern management systems are widely used, including in the management of teams of people united by common goals (organizations, departments, groups of developers, etc.). Information security is no exception - it is not enough to saturate the division responsible for information technology security with personnel, technical systems of information protection, it is necessary to ensure the effectiveness in achieving the goals, which is not possible without an appropriate management system. Information security specialists in organizations of various forms of ownership often face the problem of ensuring effective and efficient protection of information assets. Availability of international and national standards, regulatory documents of regulators does not ensure the achievement of high performance and efficiency indicators. The achievability of these indicators is determined by setting and achieving a number of goals, based on certain strategic principles of information security management system.

1. Introduction
Spring 1943. World War II is in full swing. The continuation of hostilities by one member of the anti-Hitler coalition (Great Britain) is complicated by the fact that supplies of raw materials, equipment and weapons from the United States, Canada, and Australia are needed. The situation is aggravated by the fact that the number of sunken transport ships making deliveries is increasing every month and already greatly exceeds the country’s ability to build new transport ships. The main losses of transport ships are sustained by specially organized attacks by German submarines (the "wolfpacks" scheme). Neither the technical anti-submarine systems developed and adopted before the war began - ASDIC active submarine detection sonar and the anti-submarine bomber jet ("hedgehog") - save the situation, nor the fact that all important supplies are carried by transport ships in convoys guarded by warships. With the goal of taking Great Britain out of the war, Germany continues to invest its resources in a costly strategy of submarine warfare. Although individual submarines are lost, the number of transport ships they sink more than recoups the cost. In the spring of 1943, the Kriegsmarine Command did not yet anticipate that the "battle for the Atlantic" had already been lost. From the second half of 1943 the number of transports sunk and the number of submarines destroyed began to decline. In 1945 there was an average of one sunken submarine per Allied transport sunk. Trading a cheap transport ship, even with cargo, for an expensive submarine with a professional crew is already an unacceptable loss for Germany. This result was largely due to the proper organization of the anti-submarine defense management system, which included both an organized order of convoy formation, collection and escort of stragglers and disabled ships, preliminary air reconnaissance, at least in the range of aviation in the convoy formation area, constant communication between convoys, interception and tracking of German submarine communications, orderly actions of escort ships, in case a submarine is discovered, etc. In addition, the victory in the "Battle of the Atlantic" was facilitated by the excellent organization of technology for the rapid construction of transport ships such as the Liberty. This is a historical example of a management system based on the principles of systematic, process-based, risk-oriented and proactivity, all of which make it

1 Kriegsmarine - German Navy
2 In the initial period of convoys, if a single submarine was detected, the escort ships would rush to destroy it, leaving the transports to be devoured by the other submarines of the "wolf pack. And this despite the fact that the bait submarine itself, as a rule, could not
3 The organization of construction technology and commonality (standardization) of design approaches in U.S. shipyards was such that instead of several years it took 2-3 months to build one ship (the record was 42 days)
possible for management systems to be highly performance and effectiveness in achieving their goals even today.

2. Prerequisites for the creation of the IS management system

The situation with information security (IS) in commercial companies, government and non-profit organizations is largely similar to the early stages of the "fight for the Atlantic" - there are numerous technical systems, there is experience in implementing individual IS measures, numerous IS policies have been approved, but there is no holistic IS system. The reason is the lack of an adequate IS management system.

Objectives of different organizations are different - so the main goal of commercial organizations is making a profit, increasing their value, non-profit organizations, have the goal to meet the needs of its members without making a profit, state organizations, the main most common goal is to ensure the implementation within the given competence of the state policy in the relevant sphere of functioning of the state and society. What unites these organizations that have such different goals is a single strategic objective of ensuring the continuity of their activities. Virtually any, with few exceptions, modern organization is largely, if not completely, dependent on information technology (IT).

IT continuity is essential for an organization to achieve its business goals. In turn, IT continuity is largely determined by the effectiveness of an organization’s information security (IS), because continuity of IT services, IT services and information security systems is essential to ensure availability, integrity and confidentiality. In fact, IS threats are created largely by vulnerabilities present in IT assets. The realization of IS threats leads to direct and indirect financial, reputational and other losses (including the realization of compliance risks). And losses can be catastrophic for an organization.

The modern trend of IT to expand its application in the economic, political, social and other spheres, as well as the penetration of IT into the area of human life support, only aggravates the situation. Organizations’ business processes, human life support processes are becoming increasingly vulnerable to IS threats, IS risks at the operational level are escalating to the strategic business risks of the organization, and the number of IS incidents is increasing.

Organizations create, in one form or another, an IS unit. The list of business processes includes the process of "Ensuring IS". However, this often does not guarantee that the goal of business continuity will be achieved.

3. IS management system and IS system

The retrospective of the events of the "Battle of the Atlantic" clearly shows that no matter how many technical means, personnel and other resources are involved, it is impossible to achieve the desired result unless all this is subordinated to an adequate management system. With regard to information security, it is necessary to distinguish between an information security system (ISS) and an IS management system (ISMS). The ISS is a set of protective means, measures, resource and administrative support, and the ISMS is the direct management of the ISS. In other words, the ISS is the technical subsystem of the IS, while the ISMS is the part of the organization’s management that is designed to create, implement, operate, monitor, analyze, maintain and improve the IS system. Usually there are no serious problems with the ISS because there are numerous technical systems in place, IS policies have been written, an IS unit has been established, etc. The problem, more often than not, is the weakness or complete absence of an adequate IS management system. You can invest a lot of money to buy technical systems, create a large IS department, but unless it is managed, the result will either be far from achieving the strategic goal of IS, or it will not exist at all.

4. Performance and effectiveness ISMS

Building an ISMS without the support of top management is not possible in principle. The prerogative of deciding on the allocation of resources for ISMS (financial, technical, human, etc.) belongs to the management of the organization. The role of organizational management in the creation, development and support of ISMS is described in a number of international and domestic standards, in particular in the Bank of Russia standard [4]. Performance of this role requires from ISMS to provide confidence of management in the correctness of investments in system development. Indicators that give such confidence are effectiveness and efficiency, which allow the management to assess the quantitative and qualitative indicators of ISMS. Efficiency and effectiveness are defined, for example, by GOST R ISO 9000-2015 [3] as follows:

---

4 National standard GOST R ISO/IEC 27000 - 2012 [1]
5 National standard GOST R ISO/IEC 15408 - 2012 [2]
6 In particular, violation of the requirements of federal legislation
7 Separate division or dedicated employees
8 In accordance with the quality standard GOST R ISO 9000 [3]
9 Recommended by Bank of Russia Standard STO BR IBBS-1.0-2014 [4]
- performance is the degree to which planned activities are implemented and planned results are achieved;
- effectiveness is the ratio between the achieved result and the used resources used.

Performance and effectiveness are the most important parameters of ISMS, allowing management to determine whether the cost of information security is adequate to the contribution of the IS management system to achieving the strategic goal of ensuring business continuity of the organization. These two parameters are the basis for communication in the same conceptual field of organizational management and the IS unit. The basis for ensuring the performance and effectiveness of the ISMS is a systematic approach to its organization.

**System and process approaches ISMS**

ISMS is a system. According to GOST R ISO IEC 15288-2005 [5], a system is a combination of interacting elements organized to achieve one or more goals. Consideration of a system as an integral set of elements in a set of connections and interactions between them is a system approach. This means that ISMS should be organized as a set of interrelated elements (objects, components), which has input, output, communication with the external environment, feedback. This corresponds to the concept of "process", one of the definitions of which: process is a stable and purposeful set of interconnected actions that transform inputs into outputs according to a certain technology to obtain predetermined results that are of value to the consumer. The use of the system approach implies the processuality of IS management system. ISMS at the strategic level of an organization represents a business process, which can be conventionally designated as "Ensuring IS". Achievement of the strategic goal is usually provided by a set of tasks, each of which is provided by its own subprocesses and procedures and has its own operating goals. That is, at the operational level ISMS is a set of processes of information security of the operational level (IS processes). A modern ISMS includes more than twenty IS processes.

The key ISMS indicators (performance and efficiency) largely depend on the level of maturity of IS processes, as well as a properly formed responsibility matrix. The maturity of processes is assessed within the framework of management maturity level assessment models. There are universal models (CMMI - Capability Maturity Model Integration), as well as specialized models related, for example, to IT, but which may be used to evaluate IS processes maturity as well (for example, GOST R ISO/IEC 15504 [6]). As for the responsibility matrix, of the many options (RASCI, RACI, RACIQ, etc.), the simplest option - RACI - is most often used. In such a responsibility matrix the following categories of responsibility are established - R (Responsible - direct performer), A (Accountable - responsible for the result and quality control), C (Consulted - consultant for the task, process owner, advisor), I (receiver of information / report on the completion of tasks, partner, management). However, this is not always enough. In some IS processes, for example "Awareness and Information", it is necessary to involve other departments of the organization in some of the IS processes. In this case, the function of the executor’s assistant (S - Supported) is required. Thus, it is necessary to use the RASCI model to form a responsibility matrix in ISMS.

**The risk-oriented nature of ISMS**

Any, even the smallest and insignificant, process is always associated with a number of risks, in the implementation of which, the goal of such a process is achieved partially or not achieved at all. The essence of the risk-oriented approach is to find the causes that prevent the achievement of the goals of the organization or system, prevent the normal functioning of processes, can lead the organization to failure, as well as to identify ways to reduce the impact of these causes.

Given the current trend of IT use, the increasing number of IS incidents, and the escalation of operational level IS risks to the strategic business risks of the organization, when assessing the business risks of an organization, it is necessary to compare IS risks with the strategic risks of the organization, for example, within the GRC (Governance, Risk and Compliance) concept. GRC is a universal tool designed to manage policies, risks, business continuity, incidents, compliance with standards, practices and regulatory requirements, etc., consisting of ITGRC and Financial GRC. IS Risks is part of the ITGRC (Information Technology GRC) structure, which focuses on IT-centric processes.

**Proactivity**

The concept of proactivity, as applied to security systems, is fairly new. Previously, it was used in individual technical protection systems, such as anti-virus software. One of the first areas in which proactivity...
was applied at the level of management system strategy was in the area of occupational health and safety. Nowadays, the concept of proactivity is beginning to be applied to ISMS as well.

Proactivity is based on preventive action, i.e., action taken to avoid, eliminate the cause of, or reduce the likelihood of a potential nonconformity or other potential undesirable situation.

To understand the essence of proactivity is easier on the example of its antipode - reactivity, which until recently has been the basis for corrective actions in the framework of ISMS. The initial event for changes in a reactive system is an incident. Only after that are actions taken to address the consequences, and corrective actions are developed to prevent the factors that led to the incident from occurring again. In contrast to reactivity, proactivity is based on the analysis and anticipation of risks (one of the defining moments of the need for risk-oriented ISMS), the development of appropriate prospective countermeasures.

5. Conclusions
Modern IS management system, involved in solving the most important strategic task of ensuring the continuity of the organization's business activities, should be based on the following principles:

1. the strategic goal of ISMS is to ensure the continuity of information technology used in the organization by maintaining the levels of availability, integrity, confidentiality of information assets established by management;
2. IS management system on effectiveness and efficiency in achieving the business objectives of the organization must meet the expectations of the organization management;
3. IS management system on the basis of processability shall be based on the level of effectiveness and efficiency required by the management;
4. IS management system must be risk-oriented and adequately meet the organization IS business risks;
5. one of the strategic goals of the organization's ISMS development is the transition to proactivity.

References
[1] National standard, GOST, ISO/IEC, 27000-2012, Information, technology, Methods, means, ensuring, security, Management Systems, information, General, review, terminology, approved, by Order, Federal, Agency, technical, regulation, metrology, 15.11.2012, 813-st. [Electronic resource]. Access from the legal reference system "Garant".
[2] National Standard of the Russian Federation GOST R ISO/IEC 15408-1-2012 "Information technology. Methods and means of security provision. Security assessment criteria for information technologies. Part 1. Introduction and general model": approved and put into effect by Order of Federal Agency for Technical Regulation and Metrology of November 15, 2012 N 814-st. [Electronic resource]. Access from the legal reference system "Garant".
[3] National standard of the Russian Federation GOST R ISO 9000-2015 "Quality Management Systems. Main provisions and vocabulary": approved and put into effect by the Order of the Federal Agency for Technical Regulation and Metrology from September 28, 2015 N 1390-st. [Electronic resource]. Access from the legal reference system "Garant".
[4] Bank of Russia Standard STO BR IBBS-1.0-2014 "Ensuring Information Security of Organizations of the Banking System of the Russian Federation. General provisions": adopted and enacted by the Bank of Russia on May 17, 2014 N R-399. [Electronic resource]. Access from the legal reference system "Garant".
[5] National Standard of the Russian Federation GOST R ISO/IEC 15288-2005 "Information Technology. System engineering. System lifecycle processes": approved by the Order of Federal Agency for Technical Regulation and Metrology of December 29, 2005 N 476-st. [Electronic resource]. Access from the reference and legal system "Garant".
[6] GOST R ISO/IEC 15504 "Information technologies. Process evaluation. Part 2. Assessment": approved and put into operation by the Order of Federal Agency for Technical Regulation and Metrology of December 9, 2009 N 634-st. [Electronic resource]. Access from the electronic fund of legal and normative-technical documents.

10 For example, DuPont's industrial safety methodology.
11 National Standard of the Russian Federation GOST R ISO 9000-2015 "Quality Management Systems. General provisions and vocabulary".
12 Unfortunately, the transition to proactivity has a number of serious difficulties, one of which is that it is necessary to change the overall corporate culture in the direction of making all employees aware of the need for information security.
13 Recently, organizations have begun to need to include the control of ISMS another property of information - the reliability (reliability of the source).