Куликов Даниил М03-903

**Rus-Eng 10**

**Sourcing strategy development**

After setting the targets, an enterprise has requirements for personnel. HR specialists deal with these tasks. This process includes both outsourcing, when the provider is outside, and insourcing, when the necessary goods and services are intentionally purchased or leased from the organization itself. When information security employees are distributed, a company should determine, which functions will be performed by existing or hired employees, and which functions will be performed by third party (e.g., a security service provider). Outsourcing is a common business practice involving a wide range of functions.

But despite all its advantages, outsourcing does not provide data security and system protection, especially, where regulatory compliance is an important factor.

Traditional sourcing is based on competitive bidding rituals that provide low prices and a moderate but acceptable level of quality and that are carried out with the only purpose of attracted resources cost reducing. The selected supplier gets the opportunity of doing business for a short period, and then the bidding process is repeated. For decades, this model was serving well the interests of various industries and was continuing to operate as long as costs were remaining the main driving force of sourcing. [1, 153]

However, most respondents intend to continue using outsourcing, taking into account the lessons learned from past agreements, and adopting the following rules:

* clear definition of core and strategic functions that should not be outsourced if the company wants to maintain competitive advantages;
* the signing of short-term contracts allowing its revision and abolition. A comprehensive service level agreement is mandatory; it should include both quantitative and qualitative indicators in order to provide flexibility and to avoid provider complacency;
* working with multiple providers will help maintain independence;
* standardized planning and decision making process;
* the management organization should assist with the realistic plans preparation, define clear criteria for the provider selection, and provide for the allocation of resources and time to manage the process of preparing the agreement in order to minimize operational complexity in the future [2].

As is case of any staff, the team productivity depends on many factors, including supervision. The enterprise must implement personnel policy designed and aimed at achieving success in order to create an environment where cybersecurity professionals, as well as IT operations and employees performing cybersecurity tasks, could develop.

Key features of the optimized personnel:

1. *Multitasking functionality*: the team should include employees who possess related professions in various fields of cybersecurity, thereby it provides opportunities for training, mutual support, and reduces decision-making time under crisis conditions.
2. *Ongoing training*: increasing employee productivity is achieved through resources and opportunities for training and development, what often contributes to the retention of the best specialists.
3. *Flexibility*: the ability to work in a flexible, less strictly limited environment promotes creativity, innovation and high job satisfaction.

The IT outsourcing project management involves distributing specific tasks among several providers. Such tasks include maintaining awareness of regulatory and legal issues, understanding the changing business needs, effective communication with the provider, and managing the smooth data acquisition and transfer from outsourced IT systems.

Outsourcing agreements should be reassessed periodically to ensure compliance with the amended legal and regulatory restrictions. The person or persons performing this task should be aware of both the updated information and the legislation changes. They should also be able to integrate these changes into contracts as needed.