ECONOMY AND OPERATION OF NATIONAL ECONOMY

MODERN DIRECTIONS OF INFORMATIONAL THREATS AND TRENDS OF THE INFORMATION SECURITY MARKET

Azeev A.S.
PhD student of Department of Management
and Mathematical Modeling of Market Processes,
Odesa I.I. Mechnikov National University

Chaikovska M.P.
PhD, Associate Professor of Department of Management
and Mathematical Modeling of Market Processes,
Odesa I.I. Mechnikov National University

With the development of technology, we have been increasingly observing the branching of the network perimeter, which traditionally protects the information system. Instead, such technologies as mobility, cloud computing etc. only increase the potential area for attack.

When analyzing methods used by attackers, it is important to track the changes that occur in their tactics. To do this, let us consider the new trends in the development of malicious software, web-attacks and spam, as well as the risks associated with Potentially Unwanted Software (PUA) of spyware type, Business Email Compromise (BEC), as well as changes in the economy of information crimes.

In addition to financial expenses, the greatest damage resulting from information security crimes was caused to operational and financial systems, brand reputation suffered, customers' loyalty indicators deteriorated.

The main obstacles on the way of advancement of strategic defense plans are budget restrictions, lack of system compatibility and qualified specialists. Structures of organizational subdivisions are constantly complicated. In these conditions, an assessment of the effectiveness of information security methods is a critical factor.

In order to provide the appropriate level of protection, processes and tools for collecting and analyzing data on informational threats on real-time as well as the exchange of these data between companies are required. Management of informational threats is a multisided complex process that uses several interrelated systems for collecting, collating and analyzing information about threats from different sources.

Relevant methods include the cloud model and adaptive authentication. These technologies provide a contextual approach to threats and allow understanding the tactics, methods and sequence of actions of law breakers. Moreover, the network of permanent information exchange can provide the organization of data, based on which it is possible to take specific measures, identify the company's major risks and increase the operational efficiency of detecting incidents in the field of informational, security and respond to them.