UDC 004.056:34

DEVELOPMENT AND OPERATION OF NATIONAL CYBERSECURITY SYSTEM

Shchukina A. A.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Yushkevich E.V. - lecturer of the Department of Foreign Languages

Annotation. The article is devoted to Decree No. 40 "On Cybersecurity". At the beginning of the article, the problem of cyberattacks and hacks in Belarus is underlined. Next, the basic principles of the creation and functioning of a national system of cybersecurity are explained. Finally, the article describes the main and additional information security tools for creating cybersecurity centers.

Keywords: cybersecurity, hack, cyberattack, information security, decree, cybercrime, software, hardware, cybersecurity center, Operations and Analysis Center of the President of our Republic.

Introduction. In 2020-2023, numerous websites and resources of government bodies and organizations were subjected to cyberattacks and hacks. In 2021 - website of Belarusian Nuclear Power Plant, website of Ministry of Internal Affairs of the Republic of Belarus AIS «Passport» and SIS «Population Register». In 2022 - website of Belaruskali Joint Stock, website of Belorussian-Russian Belgazprombank Joint Stock, website of Belarusian Railway and others. This year - infrastructure of the state institution "Republican Clinical Medical Center" of the Administration of the President of the Republic of Belarus and others.

These facts of cyberattacks, significant economic damage inflicted on the economy of our country, as well as the accumulated experience of specialists in combating cybercrime, became the main reasons for the signing of Decree No. 40 "On Cybersecurity".

Main part. The document regulates the basic principles of the creation and functioning of a national system for ensuring cybersecurity, which should form a comprehensive tool aimed at protecting government bodies and organizations, as well as critical infrastructure objects, from cyberattacks. According to this Decree, elements of the national cybersystem include Operations and Analysis Center of the President of our Republic, National Center of Cybersecurity, centers of cybersecurity, authorized telecommunications operator, information infrastructure objects. Under current legislation, the obligation to establish cybersecurity centers is imposed on owners of critical information infrastructure facilities, authorized internet service providers, organizations which provides hosting services for official websites and email services, and other organizations determined by the Council of Ministers of Belarus upon the proposal of the Operational and Analytical Center.

The formation of cybersecurity centers involves three stages: design, creation, and certification. The design stage includes audit of the organization's information infrastructure and development of a protection system. The stage of auditing an organization's information infrastructure includes the following analyzing the structure of the information system and information flows (internal and external) of the organization in order to determine the composition (quantity) and location of information system elements (hardware and software), its physical and logical boundaries. The stage of developing a security system comprises issuing an information security policy; defining the requirements for an information security system in the Technical Task for creating an information security system; choosing technical and cryptographic means of information security and developing a general scheme of information security system.

During the stage of creating cybersecurity centers, the tasks such as procurement and/or provision of technical and cryptographic protection tools for use through subscription or resale; installation and configuration of technical and cryptographic protection tools; debugging and verifying the correct execution of security requirements by these technical and cryptographic protection tools in real operating conditions and in interaction with other objects of information systems; providing technical support are addressed.

During the certification stage, such activities as development of a certification program and methodology, establishing compliance of the real composition and structure of objects in the information system with the general scheme of the information security system, conducting tests of the information security system to ensure compliance with the legal requirements for information protection, preparation of a technical report and testing protocol and issuance of a corresponding certificate of compliance are carried out.

The main information security tools used in the creation of cybersecurity centers include SIEM and SOAR.

SIEM (Security information and event management) is a class of software products designed to collect and analyze information about security events. SIEM systems track real-time alarm signals from network devices and applications, process the collected data, identify relationships between them, detect deviations from the normal behavior of controlled systems, and notify operators of detected incidents.

The second essential tool is SOAR. SOAR (Security Orchestration, Automation, and Response) is a toolkit that allows collecting data on security threats from various sources for subsequent analysis. The tasks of SOAR include orchestration, automating tasks based on predefined scenarios, managing cybersecurity incidents and prioritizing actions, logging actions, generating reports. Orchestration - integrating technologies and tools to make decisions based on risk level information and system status. Generating reports - visualizing information on key metrics and creating summaries for analysts, cybersecurity unit managers, and enterprise management.

Additional information security tools for creating cybersecurity centers involve VM, NAD, Next Generation Firewall, AntiDDoS, and Scan.

VM (Vulnerability Management) is a vulnerability management system that prioritizes vulnerabilities based on their level of danger to business processes and assets, and automates vulnerability management processes depending on the existing systems and their impact on the overall operation of the company.

The NAD (Network Attack Discovery) system is a deep traffic analysis system that detects attacks on the perimeter and within the network, determines what is happening in the network, detects malicious activity even in encrypted traffic, and helps with investigations. NAD's tasks include detecting malicious activity, including in encrypted traffic, identifying malware and deviations from regulatory requirements (network compliance violations), and identifying the use of remote administration protocols, anonymizers, and other data exchange standards.

Next Generation Firewall - a hardware-software complex of a new generation of firewall designed for deep traffic filtering, integrated with IDS (Intrusion Detection System) or IPS (Intrusion Prevention System), and capable of controlling and blocking traffic at the application level.

AntiDDoS - specialized software-hardware and software tools designed to protect an organization's web servers (websites) from Distributed Denial of Service (DDoS) attacks.

Scan - a vulnerability scanner, a software or hardware-software complex designed to assess the real state of information infrastructure security, identifies network components, scans network resources for vulnerabilities, and provides recommendations for their elimination.

Conclusion. In conclusion, the implementation of measures and measures provided for in the President's Decree, the competent construction and formation of cybersecurity centers using information protection means will enable efforts to be directed towards detecting, preventing, and minimizing the consequences of cyberattacks on the country's information infrastructure objects.

References

1. Decree of the President of the Republic of Belarus No.40 [Electronic resource]. – Mode of access: https://etalonline.by/document/?regnum=p32300040. – Date of access: 21.03.2023.