UDC 004.056

A.G. Korchenko, Dr Eng, Yu.A. Dreis, PhD, O.A. Romanenko
(National Aviation University, Ukraine)

Structure of the method of estimating the consequences of the leakage of state secrets from cyber attacks to critical information infrastructure

At present, considerable attention is paid to protecting the critical infrastructure of Ukraine in which widely used information technologies (IT). At the same time, IT development contributes to creating new vulnerabilities and potential threats to critical information infrastructure (CII) and especially for state secrets (SS) the disclosure of which may damage the national security of the state. Therefore, there is a need to assess the negative consequences for national security in the event of a leakage of SS. In view of this, developed the structure of method for assessing the consequences of leakage of SS from cyber attacks to the CII of the state. Which, with the help of the specified parameters, will enable to assess the consequences of the leakage of SS, both within individual regions and for the state as a whole.

Structure of the method of estimating the consequences of the leakage of state secrets from cyber attacks to critical information infrastructure.

The structure of the method for assessing the consequences of a state secrets (SS) leak includes six steps, each of which has a certain number of steps.

Stage 1. Formation of the set of data-identifiers of the subject of regime-secret activity (SRSA) - the object of critical infrastructure (OCI).

This stage defines all the information specified by the regulatory documents, about SRSA - OCI. At each step defined information about the name, location, ownership, information about the institution, providing access and allowing employees and other data that will assess the situation at the facility. The information is determined by the formula in the general case, i.e., when changing the data, the formula does not change. Below are all steps in the first stage.

Step 1.1 The full name of OCI and the code of the Unified State Register of Enterprises and Organizations of Ukraine (USREOU).

Step 1.2 Location of OCI, legal and postal address.

Step 1.3 Form of ownership of OCI .

Step 1.4 Data about the higher level institution (subordination).

Step 1.5 Data about the permission to conduct activities related to SS.

Step 1.6 Data on the number of Material carriers of secret information (MCSI), MCSI with the fingerboard of secrecy of other states (entities), the transfer of classified information to other states (entities), and identification of those MCSI on which violations occurred.

Step 1.7 Data about the availability of employees and access to SS.

Step 1.8 Data on secret Research and Development (R&D).

Step 1.9 Data about regime-secret objects (RSO), financing of means of protection of SS (PSS).

Stage 2. Qualification of violations in the area PSS.

The next stage is to display information about violations that have been detrimental to national security in the area PSS. The stage consists of three steps that determine the violation, the level of criticality and what information has been disclosed.

Step 2.1 Establishing the fact of detected potential violation and the object of critical information infrastructure (OCII).

Step 2.2 Identification OCII on OCI and the level of their criticality - regime rooms, objects of informational activity.

Step 2.3 Identification of the data (information) constituting the SS regarding which the violation occurred.

Stage 3. Assessing the security of SS on OCI.

The third stage determines at what level was the protection of the OCI and the effectiveness of the implemented protection measures. This stage includes six steps that reveal the assessment of the security of the SS on the OCI.

Step 3.1 Determination of the coefficients of the importance of the data regarding which the violation occurred.

Step 3.2 Determination of the coefficients of the importance of possible threats (cyber-threats) with PSS.

Step 3.3 Determination of the list of tasks and methods (means) of PSS for elimination of threats (cyber-threats).

Step 3.4 Determination of the effectiveness of the measures taken to protect the SS in the OCI.

Step 3.5 Calculation of the efficiency of the system of PSS on OCI.

Step 3.6 Determination of the level of protection of SS on OCI.

Stage 4. An expert assessment of the importance of data about which violations occurred.

The next stage determines the evaluation of the data that forms the SS for which the violation occurred. The fourth stage includes seven steps, which reveal additional parameters for the violation of the leakage of data constituting state secrets, which will allow to evaluate the consequences in full.

Step 4.1 Evaluate the importance of the date for the OCI and the SS area as a whole.

Step 4.2 Determining the proportion of the object of the data

Step 4.3 Identification of the components of the object of the data and defasification of the linguistic variable.

Step 4.4 Determination of the level of reduction of the effectiveness of OCI activities associated with SS.

Step 4.5 Establishing the relative magnitude of damage to the degree of secrecy of the data that make up the SS.

Step 4.6 Determining possible other grave consequences and determining the relative magnitude of damage.

Step 4.7 Calculation of the coefficient of moral aging of data constituting SS for which there was a violation.

Stage 5. Assessment of negative consequences caused by violation.

The next stage is a direct assessment of the negative consequences or damage to the national security of Ukraine committed in violation. This stage consists of six steps, which determine the cost of realized methods/means of protecting SS, economic and total damage.

Step 5.1 Calculation of financing of measures for PSS.

Step 5.2 Calculation of cost MCSI which are registered and stored in OCI.

Step 5.3 Calculation of cost OCII and implemented in them methods (means) of the PSS.

Step 5.4 Calculation of the magnitude of the economic damage caused by the violation.

Step 5.5 Calculation of the magnitude of economic damage to other grave consequences of the violation.

Step 5.6 Assessment of the negative consequences (total damage) caused by the violation.

Stage 6. Assessment of negative consequences caused by violations in the field of PSS within the occupied territory or in the area of an Anti-Terrorist Operation (ATO or Joint Forces Operation (JFO)), region or state as a whole.

The final stage determines the general harm to national security from violations in the sphere of PSS within the limits of a separate territory or state as a whole.

Step 6.1 Conducting an assessment of the negative consequences of violations by each SRSA within a defined territory.

Step 6.2 Calculation of negative consequences (total damage) by the SRSA where there was a violation in the field of protection against the level of terrorist threats in the area of ATO (JFO).

Step 6. Calculation of negative consequences (total damage) for the SRSA where the violation occurred in the area of protection within the occupied territory, region or state as a whole.

Step 6.4 Summarizing the data and forming an expert opinion on the assessment of the consequences of the leakage of SS from cyber attacks to the critical information infrastructure of the state.

Therefore, the structure of the method of estimating the consequences of leakage of SS from cyber attacks to CII has been developed. Which will give an opportunity to reveal the essence of the method of assessing the consequences of the leakage of SS from the violation in the sphere of PSS, both within a separate territory and for the state as a whole.

References

1. Korchenko O., Arkhipov O., Dreis Yu., “Assessment of damage to the national security of Ukraine in the event of leakage of state secrets: a monograph”, K .: Sci. Center on the Security Service of Ukraine, 332 p., 2014, ISBN 978-617-7092-26-0.

2. Korchenko A., Dreis Yu., Roshchuk M., Romanenko O. Consequence evaluation model of leak the state secret from cyberattack directing on critical information infrastructure of the state // Ukrainian Scientific Journal of Information Security, 2018, vol. 24, issue 1. – P. 29-35.

3. Dreis Yu., “Analysis of basic terminology and negative consequences of cyberattacks on snformation and telecommunication systems of state critical infrastructure facilities,” Information Protection 19 (3), pp. 214 – 222, 2017.