Svitlana KAZMIRCHUK[1], Yurii DREIS[2], Ynina ROI[3],
Olha ROMANENKO[4]

Scientific supervisor: Alexander KORCHENKO[5]

AN ASSESSMENT OF THE CONSEQUENCES OF THE LEAKAGE OF STATE SECRET FROM CYBERATTACKS TO A CRITICAL INFRASTRUCTURE

Abstract: 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 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 state secrets. In view of this, developed the structure of method for assessing the consequences of leakage of state secrets 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 state secrets, both within individual regions and for the state as a whole.

Keywords: problems, critical infrastructure, protection of objects of state's critical infrastructure, cyber attack.

OCENY KONSEKWENCJI WYCIEKU TAJNYCH INFORMACJI PAŃSTWOWYCH Z POWODU CYBERATAKÓW NA INFRASTRUKTURĘ KRYTYCZNĄ PAŃSTWA

Streszczenie: Obecnie wiele uwagi poświęca się ochronie infrastruktury krytycznej Ukrainy, w której szeroko stosowane są technologie informacyjne. Jednocześnie rozwój technologii informatycznych przyczynia się do nieumyślnego tworzenia nowych słabych punktów i potencjalnych zagrożeń dla krytycznej infrastruktury informacyjnej (KII), a zwłaszcza tajemnic państwowych, których ujawnienie może zaszkodzić bezpieczeństwu narodowemu

[1] Dr Eng (Information security), Head of Computerized Information Security Systems Academic Department, National Aviation University, sv.kazmirchuk@nau.edu.ua
[2] PhD Eng (Information security), Head of Innovative Technologies Professional Education Academic Department, National Aviation University, Dreisyuri@gmail.com
[3] PhD Eng, Associate Professor of Department of Information and Cybernetics, Borys Grinchenko Kyiv University, y.roi@kubg.edu.ua
[4] Student, Insitute of Computerized Information Systems, Academic Department of Computerized Information Security Systems, National Aviation University, olya_olek@ukr.net
[5] Dr Eng (Information security), Professor, Laureate of the State Prize of Ukraine in Science and Technology, Head of IT-Security Academic Department, National Aviation University, Visit-Professor at The University of Bielsko-Biala, Leading Researcher of the National Academy of State Secret of Ukraine, icaocentre@nau.edu.ua

państwa. Dlatego istnieje potrzeba oceny negatywnych konsekwencji dla bezpieczeństwa narodowego w przypadku wycieku tajemnicy państwowej. W związku z tym opracowano strukturę metody oceny skutków wycieku tajemnic państwowych z cyberataków na KII państwa. Które przy pomocy określonych parametrów umożliwią ocenę konsekwencji wycieku tajemnic państwowych, zarówno w obrębie poszczególnych regionów, jak i państwa jako całości.

Słowa kluczowe: kodowanie typu 'tuple' tzw. n-tki, infrastruktura krytyczna, ochrona obiektów infrastruktury krytycznej państwa przed cyberatakiem

1. Introduction

Due to the rapid development of information technologies in all spheres of human and state life support, it has increased the requirements for the protection of information and telecommunication systems. The critical infrastructure of Ukraine has become an exception. Which requires first-priority protection and assessment of losses in the event of loss or disclosure of state secrets. As this may harm the security and vital interests of the state [1]. Therefore a tuple approach was developed to assess the consequences of the state secrecy leak from cyber attacks to critical infrastructure. Which consists of six stages.

2. Stages of assessing the consequences of the leakage of state secret from cybercasts to critical information infrastructure

The tuple approach for assessing the consequences of a state secrets 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 mode-secret activity (SMSA) - the object of critical infrastructure (OCI)

This stage defines all the information specified by the regulatory documents, about SMSA - 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.
Information about OCI/SMSA of his subordination and departmental affiliation **IS** (*Information about the Subject*) will be reflected in the tuples:

$$\mathbf{IS} = \langle \mathbf{IS}_1, \mathbf{IS}_2, ..., \mathbf{IS}_i, ..., \mathbf{IS}_k \rangle, \quad (1)$$

where $\mathbf{IS}_i \subseteq \mathbf{IS}$ $(i=\overline{1,k})$ - the tuple component representing the *i*-th object identifier, *k* is their number, and for all members **IS** a characteristic property of the order, where each of the identifiers corresponds to the sequence of steps in the stage.
For example, $k=9$ $(i=\overline{1,9})$ formula (1) will look like:

$$\mathbf{IS} = \langle \mathbf{IS}_1, \mathbf{IS}_2, \mathbf{IS}_3, \mathbf{IS}_4, \mathbf{IS}_5, \mathbf{IS}_6, \mathbf{IS}_7, \mathbf{IS}_8, \mathbf{IS}_9 \rangle =$$
$$\left\langle \begin{matrix} (\mathbf{IS}_{11}, \mathbf{IS}_{12}), \mathbf{IS}_2, \mathbf{IS}_3, (\mathbf{IS}_{41}, \mathbf{IS}_{42}, \mathbf{IS}_{43}), (\mathbf{IS}_{51}, \mathbf{IS}_{52}, \mathbf{IS}_{53}), (\mathbf{IS}_{61}, \mathbf{IS}_{62}, \mathbf{IS}_{63}, \mathbf{IS}_{64}, \mathbf{IS}_{65}, \mathbf{IS}_{66}), \\ (\mathbf{IS}_{71}, \mathbf{IS}_{72}, \mathbf{IS}_{73}, \mathbf{IS}_{74}, \mathbf{IS}_{75}, \mathbf{IS}_{76}, \mathbf{IS}_{77}), (\mathbf{IS}_{81}, \mathbf{IS}_{82}, \mathbf{IS}_{83}, \mathbf{IS}_{84}), (\mathbf{IS}_{91}, \mathbf{IS}_{92}, \mathbf{IS}_{93}) \end{matrix} \right\rangle =$$
$$\left\langle \begin{matrix} (N, CD), U, O, (SU, CO, CU), (NP, DP, VP), (DC, MCE, MCT, MCF, SS, MCS), \\ (NES, NEP, FA, NEF, NESS, NPGA, NEA), (NSP, NPW, NP, NPP), (NSE, NA, FMP) \end{matrix} \right\rangle$$

(2)

Where:
N (*Name*) is defined by the plurality of names of organizations-owners /managers of ITS as OCI [2];
CD (*Code*) will determine a plurality of unique identifiers of a legal entity in the EDRPOU (National State Registry of Ukrainian Enterprises and Organizations) of the organizations-owners/managers of the ITS as OCI;
U (*Units*) - the number of locations of the OCI-SRSA, the administrative-territorial units of Ukraine, within which there is an object/entity in accordance with [2];
O (*Ownership*) ownership form of the organization-owner/manager of the ITS taking into account [3];
SU (*Subordination*) – displays a plurality of names and addresses of the organization (institution) that is directly subordinated to the OCI;
CO (*Coordinator*) – displays the name and address of the public authority in the field of management which is coordinated and coordinated by the OCI through the relevant minister;
CU (*Customer*) – displays the name and address of the customer of the secret works.
NP (*Number Permission*) – permission number;
DP (*Date Permission*) – date of the permit;
VP (*Validity Period*) – validity period of the permit;
DC (*Degrees of Secrecy*) – displays a set of vultures (degrees) of secrecy of material carriers (information);
MCE (*Material Carriers by the End*) – the number of Material Carrier of Classified Information (MCCI) at the end of the reporting period;
MCT (*Material Carriers which are Transferred*) – the number of MCCI transmitted to foreign states and international organizations in the reporting period;
MCF (*Material Carriers to Foreign Countries*) – the number of Material Carrier of Information (MCI) with denominations for restricting access to foreign states and international organizations;
SS (*Stamp of Secrecy*) – the set of access barriers of the former USSR;
MCS (*Material Carriers of the USSR*) – the number of the number of MCI with the stamps of access restrictions of the former USSR;
NES (*the Number of Employees according to the Staff list*) – total number of employees according to staff list;
NEP (*Number of Posts*) – the total number of posts included in the nomenclature of posts;
FA (*Form of Admission*) – form of admission;
NEF (*Number of posts what Form of admission*) – the number of posts included in the nomenclature of positions with the form of admission;

NESS (*the Number of Employees who have access to State Secrets*) – number of employees who have access to the state secret;
NPGA (*Number of People who have been Granted Access*) – the number of persons who were granted access to state secrets in accordance with the procedure established by law without issuing admission to state secrets;
NEA (*the Number of Employees who are Acquainted with secret information*) – the number of employees who became familiar with classified information in other enterprises, institutions, organization;
NSP (*Number of Secret Projects*) – number of secret research works, research and development works and design work;
NPW (*Number of Parts of the secret Works*) – the number of components of secret research, research and development works and design work;
NP (*Number of secret Products*) – number of secret products;
NPP (*Number Parts of the secret Products*) – the number of parts of the secret products;
NSE (*Number State of Employees*) – headcount mode-secret objects (MSO) or the number of responsible persons have a duty to ensure secrecy;
NA (*Number of Authorized*) – number of authorized persons MSO;
FMP (*Financing of Measures Protection*) – financing of measures to protect state secrets in the reporting period.

Stage 2. Qualification of violations in the field of state secrets

The next stage is to display information about violations that have been detrimental to national security in the area protection of state secrets (PSS). The stage consists of three steps that determine the violation, the level of criticality and what information has been disclosed.
Information on the qualification of violations in the area of PSS will be determined by the **QV** (*Qualification of Violations*) identifier and displayed in the tuples:

$$\mathbf{QV} = \left\langle \mathbf{QV}_1, \mathbf{QV}_2, ..., \mathbf{QV}_i, ..., \mathbf{QV}_q \right\rangle, \tag{3}$$

where $\mathbf{QV}_i \subseteq \mathbf{QV}$ $(i = \overline{1,q})$ - the tuple component that displays the *i*-th violation ID, q their number, and for all members **QV** the characteristic property of the order is characteristic, where each of the identifiers corresponds to the sequence of steps in the stage.
For example, $q = 3$ $(i = \overline{1,3})$ formula (4) will have the form:

$$\begin{gathered} \mathbf{QV} = \left\langle \mathbf{QV}_1, \mathbf{QV}_2, \mathbf{QV}_3 \right\rangle = \\ \left\langle (\mathbf{QV}_{11}, \mathbf{QV}_{12}, \mathbf{QV}_{13}), (\mathbf{QV}_{21}, \mathbf{QV}_{22}), \mathbf{QV}_3 \right\rangle = \\ \left\langle (\mathbf{FDD}, \mathbf{FLC}, \mathbf{FLI}), (\mathbf{NRR}, \mathbf{NCO}, \mathbf{NCS}), \mathbf{D} \right\rangle, \end{gathered} \tag{4}$$

where **FDD** (*Facts Disclosure Date*) – the number of facts disclosure of information constituting state secrets;
FLC (*Facts of the Loss of Carriers*) – number of facts of loss MCCI;

FLI (*Facts Disclosure Information*) – the number of facts disclosure of information with limited access by foreign states or international organizations and the loss of its MCI;
NRR (*Number of Regime Rooms*) – plenty of rooms;
NCO (*Number of Certified Objects*) – number of certified objects of informational activity, suitable for the circulation of linguistic confidential information;
NCS (*Number of Certified information Systems*) – number of certified information, telecommunication and information and telecommunication systems suitable for the circulation of classified information;
D (*Data*) **–** a set of information in the form of the article number of the On Approval of the Statement of State-Owned Information regarding a potential violation [3].

Stage 3. Estimation security of state secret on the object of critical infrastructure

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

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 state secret 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 state secret, economic and total damage [4-5].
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 state secret from cyber attacks to the critical information infrastructure of the state.
Therefore, the structure of the method of estimating the consequences of leakage of state secret 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 state secret from the violation in the sphere of PSS, both within a separate territory and for the state as a whole.

CONCLUSIONS

Thus in the work a tuple approach for assessing the consequences of the leakage of state secrets from cyber attacks to critical information infrastructure has been developed. Which will give an opportunity to reveal the essence of the method of assessing the consequences of the leakage of state secrets from the violation in the sphere of protection of state secrets, both within a separate territory and for the state as a whole.

REFERENCE

1. Verkhovna Rada of Ukraine: On the Fundamentals of National Security, Law of 19.06.2003. № 964 URL: *http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=964-15*
2. KORCHENKO A., DREIS Y., ROMANENKO O., BYCHKOV V.: The model of objects classifier of critical information infrastructure of the state. Kyiv 20(2018)1, 5-11. URL: *http://jrnl.nau.edu.ua/index.php/ZI/article/view/12448/17028*
3. KORCHENKO A., DREIS Y., ROMANENKO O.: Formation of a set of identifiers for the classification of objects of critical information infrastructure. Kyiv, 2018, 81-86. URL: *http://dspace.nau.edu.ua/handle/NAU/32648*
4. DREIS Y.: Comparative analysis of the negative effects of cyber attacks on the critical information infrastructure of different countries. Kropivnitsky, 2017, 40-43.
5. DREIS Y., MOVCHAN M.: Analysis of the negative effects of cyber attacks on information resources of critical infrastructure of the state. Kyiv, 2017, 71-74.