МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ФРАНКА
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

ITSec-2024

Безпека інформаційних технологій

МАТЕРІАЛИ

XIII Міжнародної науково-технічної конференції

9-11 травня 2024
м. Львів (Україна)

УДК [003.26+004+519.816]:004.056:65(063)

ITSec: Безпека інформаційних технологій: матеріали XIII Міжнар. наук.-техн. конф., м. Львів, 9-11 трав. 2024 р. Л.: ЛНУ ім. І. Франка, 2024, 265 с.

Збірник містить тексти наукових матеріалів доповідей та тез учасників XIII міжнародної науково-технічної конференції «ITSec: Безпека інформаційних технологій». Основною метою конференції є ознайомлення з сучасними досягненнями та висвітлення результатів наукових досліджень з усіх аспектів кібербезпеки та захисту інформації.

Призначено вченим, інженерам, аспірантам наукових спеціальностей 05.13.21 – Системи захисту інформації, 21.05.01 – Інформаційна безпека держави, здобувачам вищої освіти за спеціальностями: 125 – Кібербезпека та захист інформації, а також всім зацікавленим.

Analysis of methods and models for assessing the consequences of the loss information with limited access, its value and aging

UDK 004.056.5

Yurii Dreis[1], Oleksandr Korchenko[2]

Mariupol State University, [1]y.dreis2@mu.edu.ua, State University of information and telecommunication technology, [2]icaocentre@nau.edu.ua

The question of determining the negative consequences of the leakage of information with limited access (IwLA) for a person, society or the state always arises when establishing disciplinary, administrative and criminal liability for the fact of violation of the legislation that provides for its protection. The application of criminal charges and penalties for leaking IwLA depends on its type (confidential, official, secret) in relation to which such a violation occurred. But when resolving a legal dispute, the issue of determining the type of (moral, material, etc.) damage and, especially, the amount of damage (damage) or other serious consequences to a person, society or the state caused by such as leak of information with limited access, appears to be fairly fair, for application of an equivalent with t of compensation for these consequences. Therefore, the task of developing methodology, system methods, methods and models for assessing the negative consequences of leaking IwLA, its value and aging is urgent.

The *purpose of the work is* to research the existing methods and models for determining (evaluating) the negative consequences of the leakage of IwLA and its value according to such criteria as: 1) by type of personal data: confidential or personal data / official / secret; 2) in violation of the main properties of information security: confidentiality / integrity / availability; 3) according to the availability of damage assessment scales: linguistic / point / monetary; 4) by classification of the type of violation: disclosure / loss / leakage of information; 5) by determining the value / aging of information; 6) by place of information processing: system (ICS, CSPI) / institution (SE or PE, SRSA, OCI); 7) according to the presence of a classification of importance levels; 8) by quantitative / qualitative characteristics; 9) taking into account the requirements of domestic / international legislation.

In the table 1 provides a brief comparative analysis of the existing domestic methods and models for assessing the negative consequences of the leakage of IwLA, its value and aging [1-13] with regard to taking into account the list of the above-mentioned criteria 1)-9).

Table 1

Analysis of methods and models

Criteria → *Methods and models in works ↓*	1)	2)	3)	4)	5)	6)	7)	8)	9)
O.Arkhypov, et al. [1-3]	+/+/+	+/-/-	+/+/+	+/+/+	+/+	-/+	+	+/+	-/+
O. Korchenko [4, 5], Yu. Dreis [6, 7]	+/+/+	+/+/+	+/+/+	+/+/+	-/+	+/+	+	+/+	+/-
O. Boichenko, et al. [8, 9]	+/+/+	-/-/-	+/+	-/-/-	+/-	-/+	+	+/+	+/-

V. Shulha, et al. [10]	+/-/-	+/-/-	+/+/+	-/+/+	+/-	+/+	+	+/+	-/+
V. Zaiats, et al. [11], B. Moroz, et al.[12]	-/-/-	-/-/-	+/-/-	-/-/-	+/+	+/-	-	+/+	-/-
L. Skachek [13], M. Losev [14]	-/-/-	-/-/-	-/+/-	-/-/-	+/+	+/-	-	+/-	-/-
other [15]	-/-/+	-/-/-	-/+/+	-/-/-	-/-	-/+	+	+/+	+/-

Conclusion. The analysis showed that currently there is no universal method or model that would fully take into account all the criteria by which they were compared, and therefore has further perspective and scientific innovation in the development of new methods and models, improvement of existing ones and their further development.

1. O. Arkhypov, et al. Estimation of Efficiency of System of Protection of the State Secret. Monograph, NASSU (2007),
2. O. Arkhypov, et al. Criteria for Determining the Possible Harm to National Security of Ukraine if Disclosure Information Protected by State. Monograph, NASSU (2011).
3. O. Arkhypov, On some aspects of determination of confidential information value. Legal, regulatory and metrological support of information security system in Ukraine, (2010), 19-25.
4. O. Korchenko, Yu. Dreis, et al. Method of Fuzzy Classification of Information with Limited Access. 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020). Kyiv, Ukraine, 255-259.
5. O. Korchenko, O. Arkhypov, Yu. Dreis, Assessment harm to the Ukraine national security in case of leakage state secrets. Monograph, NASSU (2014).
6. Yu. Dreis, et al. Restricted Information Identification Model. CEUR 2022, Vol. 3288: Cybersecurity Providing in Information and Telecommunication Systems, 89-95.
7. Yu. Dreis et al. Model to Formation Data Base of Internal Parameters for Assessing the Status of the State Secret Protection, in: Cybersecurity Providing in Information and Telecommunication Systems, Vol. 3654 (2024), 277–289.
8. O. Bojchenko, et al. Mathematical model of calculation the value of information of the institution. Problems of construction, testing, application and operation of complex information systems, (2022), 30–40.
9. O. Boichenko, et al., The method of assessing the value of information. Radio electronics, computer science, control, №4 (2023), 107.
10. V. Shulha, et al., A multiple-theoretical GDPR-model of parameters for personal data. Ukrainian Information Security Research Journal, Vol.25, №4 (2023), 254-268.
11. V. Zaiats, et al. Figurative approach to the quantitative evaluation of the value of information. Dopov. Nac. akad. nauk Ukr. (2018) № 6, 32-39.
12. B. Moroz, et al., Methods of determining the value of information for the organization of its protection. Legal, regulatory and metrological support of information security system in Ukraine, №2 (2001), 46-53.

13. L. Skachek, The value of information in information security. Information security, №1 (9), 2013, 152-154.
14. M. Losev, Ovalue and aging evaluation of information with a centralized method of network manage. Science and Technology of the Air Force of Ukraine, №2 (2021), 140-144.
15. Methodical recommendations to state experts on secrets on determining the grounds for classifying information as a state secret and the degree of their secrecy. State Committee of Ukraine for State Secrets, Collection, № 8 (1998).