РЕЗІЛЬЄНТНІСТЬ ЕЛЕКТРОННИХ АРХІВІВ

Ланде Д. В.[1], Цирульнєв Ю. Б.[1]

[1]*Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м. Київ, Україна*

Доповідь присвячено аналізу резільєнтності електронних архівів як інформаційних систем. На підставі визначень резільєнтності інформаційних систем згідно міжнародних стандартів та наукових досліджень наведена математична формалізація резільєнтності, введені, визначені та математично формалізовані критерій резільєнтного перерізу (Resilience Threshold Function) та функція відновлення (Recovery Function).

Ключові слова: електронні архіви, резільєнтність, кібербезпека

Вступ

Резільєнтність є критичною властивістю сучасних електронних архівів (Digital Archives, DA) - інформаційних класу Enterprise Content Management (ECM) і Content Service Platform (CSP) [4]. У глобальному цифровому середовищі, де електронні архіви стають не лише місцем довготривалого збереження електронних копій документів, фото-кіно-відео-аудіо матеріалів та їх метаданих, а й інструментами аналізу великих обсягів інформації, активними компонентами інформаційної інфраструктури держави, забезпечення їх резільєнтності є необхідною умовою кібербезпеки, стабільності державних процесів та підтримки національної стійкості.

Наукова новизна дослідження полягає у формулюванні і математичній формалізації резільєнтності електронних архівів. Резільєнтність (Resilience) інформаційних систем - здатність адаптуватися та реагувати на вплив кіберзагроз та відновлювати свою цілісність і функціональність після кібер-інцидентів, впливу техногенних катастроф,

надзвичайних ситуацій і воєнних дій визначено стандартами [8], [9]. Інформативно зазначимо, що живучість (Survivability) інформаційних систем – здатність зберігати критично важливі функції в умовах впливу кіберзагроз, у разі пошкоджень, атак, під впливом ворожого або деструктивного середовища досліджена, визначено і формалізовано, як властивість інформаційних систем, наприклад, в роботах [3], [5], [6], [7] тощо. В даному досліджені автор пропонує формалізовану математичну модель оцінки резільєнтності електронних архівів.

Резільєнтність R_{DA} електронного архіву *DA* в умовах впливу кіберзагроз *FT* (Function Threat) $FT_{DA} = \{FT_{DA1}, FT_{DA2}, ..., FT_{DAn}\}$ залежить від наступних властивостей електронного архіву: A_{DA} – здатності *DA* передбачати вплив кіберзагрози; W_{DA} – здатності *DA* витримувати вплив кіберзагроз; Rc_{DA} – здатності *DA* відновлюватися після впливу кіберзагроз; Ad_{DA} – здатності адаптуватися до впливу кіберзагроз $R_{DA} = f(A_{DA}, W_{DA}, Rc_{DA}, Ad_{DA})$. При цьому, зазначимо, що живучість S_{DA} електронного архіву *DA* буде визначена як:

$$S_{DA} = \lim_{t \to 0} P\left[F(t) \geq F_{\min} \mid \exists D(t)\right],$$

де *F(t)* – функціональність електронного архіву; $F_{\min}$ – це мінімально допустимий рівень функціональності, який повинен забезпечити електронний архів *DA*, щоб вважатися "живим"; *D(t)* – наявність деструктивного впливу на систему в момент часу *t*; $\lim_{t \to 0}$ – межа у часі, що показує довгострокову здатність до виживання; *P*[.] – ймовірність, що функціональність не впаде нижче критичного рівня за умов наявного деструктивного впливу.

Математична формалізація резільєнтності електронних архівів може бути представлена, як базова формула резільєнтності в часі *t:*

$$R(t) = w_1 \cdot A_{AD}(t) + w_2 \cdot W_{AD}(t) + w_3 \cdot Rc_{AD}(t) + w_4 \cdot Ad_{AD}(t),$$

де $w_i \in [0,1]$, $\sum_{i=1}^{4} w_i = 1$, а також, як альтернативна нормативна формула (через інтеграл ефективності - здатність системи зберігати ефективність функціонування електронного архіву протягом інциденту та після нього):

$$R = \frac{1}{T}\int_0^T \frac{F(t)}{F_{nom}} dt,$$

де R – інтегральна резільєнтність за період спостереження T (який включає інцидент, реакцію, відн овлення); $F(t)$ – фактична функціональність електронного архіву в часі t; F_{nom} – номінальна (еталонна) функціональність. В такому разі, електронний архів вважається резільєнтним, якщо в часі $t \in [t_0, t_1]$ виконується умова $F(t) \geq \theta \cdot F_{nom}$, $\forall t \in [t_0, t_1]$, де $\theta \in [0,1]$ – мінімальний допустимий рівень функціонування під час або після інциденту – критерій резільєнтного перерізу (Resilience Threshold Function), а функція відновлення (Recovery Function) може бути представлена, як:

$$Rc(t) = \frac{F(t) - F_{\min}}{F_{nom} - F_{\min}},$$

де $F_{\min}$ – мінімальна критична функціональність; $Rc(t) \in [0,1]$ – нормована швидкість, або ступінь відновлення електронного архіву.

Графік на рис. 1 ілюструє вплив інциденту, падіння функціональності та поступове відновлення до початкового рівня:

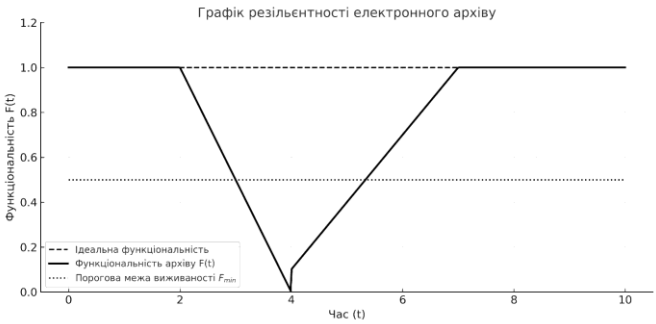

Рисунок 1. Графік резильєнтності електронного архіву

Висновки

У роботі було проаналізовано поняття резільєнтності електронних архівів у контексті міжнародних стандартів і сучасних досліджень; введено та формалізовано критерій резільєнтного перерізу (Resilience Threshold Function) та функцію відновлення (Recovery Function); запропоновано базову та нормативну математичну модель оцінювання резільєнтності електронних архівів. Майбутні дослідження у цьому напрямку можуть бути спрямовані на розробку математичних, технічних інтелектуальних методів кібербезпеки, а саме – підвищення резільєнтності електронних архівів.

Список використаних джерел

1. ISO. *Security and resilience – Organizational resilience – Principles and attributes* (ISO 22316:2017). Geneva: International Organization for Standardization, 2017. 16 p. Available at: https://www.iso.org/standard/50053.html

2. Ross R., Pillitteri V., Saydjari O., Graubart R., McEvilley M. *Developing Cyber Resilient Systems: A Systems Security Engineering Approach*. Gaithersburg, MD: National Institute of Standards and Technology, 2021. 236 p. (NIST SP 800-160, Vol. 2 Rev. 1). DOI: 10.6028/NIST.SP.800-160v2r1

3. Додонов А. Г., Ланде Д. В. *Живучесть информационных систем*. – Київ: Наукова думка, 2011. – 256 с. ISBN 978-966-00-1145-7

4. Gartner. (2017). *Definition of Content Services Platform (CSP)*. Retrieved from https://www.gartner.com/en/information-technology/glossary/content-services-platform-csp

5. Knight, J. C., Strunk, E. A., & Sullivan, K. J. (2000). Towards a Definition of Survivability. *Proceedings of the 2000 Workshop on New Security Paradigms*, 31–34. https://www.researchgate.net/publication/2397669_Towards_A_Definition_Of_Survivability

6. Ellison, R. J., Linger, R. C., Longstaff, T., Mead, N. R., & Lipson, H. F. (1999). Information Systems Survivability: Protecting Critical Systems. *Proceedings of the 1999 National Information Systems Security Conference*, 314–325, https://csrc.nist.rip/nissc/2000/proceedings/papers/314.pdf

7. Lipson, H. F. (2000). Survivability – A New Security Paradigm. *Carnegie Mellon University Software Engineering Institute*. https://www.dependability.org/wg10.4/meeting38/05-Lipso.pdf

8. NIST SP 800-160 Vol. 2 Rev. 1, Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. National Institute of Standards and Technology. DOI: 10.6028/NIST.SP.800-160v2r1

9. International Organization for Standardization. *ISO 22316:2017. Security and resilience – Organizational resilience – Principles and attributes*. Geneva: ISO, 2017. 10 p. https://www.iso.org/standard/50053.html

10. Knight J.C., Strunk E.A., Sullivan K.J. *Towards a rigorous definition of information system survivability*. // Proceedings of the DARPA Information Survivability Conference and Exposition (DISCEX 2003). Vol. 1. – IEEE, 2003. – P. 78–89. – DOI: 10.1109/DISCEX.2003.1194875

11. Ланде Д.В., Цирульнєв Ю.Б. Кібербезпека процесів інтелектуальної агрегації інформації в електронні архіви. – 2025.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ «КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»

НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

THEORETICAL AND APPLIED CYBERSECURITY

Матеріали III Всеукраїнської науково-практичної конференції

Випуск 3

Київ – 2025

Рекомендовано до друку Вченою радою
КПІ ім. Ігоря Сікорського
(протокол № 8 від 08 вересня 2025 р.)

Theoretical and Applied Cybersecurity. Матеріали III Всеукраїнської науково-практичної конференції (TACS-2025). – Київ: Політехніка. – 320 с.

До збірника увійшли матеріали доповідей, представлених на III Всеукраїнській науково-практичній конференції Theoretical and Applied Cybersecurity (TACS-2025, 29 травня 2025 р., м. Київ, Україна).

У збірнику представлені матеріали, присвячені питанням безпечного функціонування кіберпростору, безпеки промислових систем та систем критичної інфраструктури, криптографічних проблем кібернетичної безпеки, запобігання і протидії кібератакам, моделювання та протидії інформаційним операціям, технологій інформаційно-аналітичних досліджень на основі відкритих джерел інформації, застосування штучного інтелекту тощо.

Наведені матеріали з актуальних проблем інформаційної та кібернетичної безпеки, можливості застосування штучного інтелекту, системного аналізу при забезпеченні підтримки прийняття рішень, комп'ютерного моделювання процесів і систем.

Для фахівців у сфері інформаційних технологій, інформаційної і кібернетичної безпеки, а також для аспірантів і студентів старших курсів вищої школи відповідних спеціальностей.