СПИСОК ДЖЕРЕЛ ІНФОРМАЦІЇ

1. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. 3rd ed. – Wiley, 2020. – 1232 p.
2. Trend Micro. *Cybersecurity Report 2023*. – Tokyo: Trend Micro, 2023. – 116 p.
3. McAfee. *Global Threat Report 2022*. – Santa Clara: McAfee, 2022. – 101 p.
4. Stallings W. Network Security Essentials: Applications and Standards. 7th ed. – Pearson, 2022. – 592 p.
5. Bishop M. *Computer Security: Art and Science*. 2nd ed. – Addison–Wesley, 2018. – 1368 p.
6. Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. 20th Anniversary ed. – Wiley, 2015. – 784 p.
7. Хакінг та кіберзагрози: сучасні виклики безпеці. – К.: Наукова думка, 2021. – 312 с.
8. National Institute of Standards and Technology (NIST). *Framework for Improving Critical Infrastructure Cybersecurity*. Version 1.1. – Gaithersburg, MD: NIST, 2018. – 55 p.
9. FireEye. *Mandiant Security Effectiveness Report 2022*. – Reston: FireEye, 2022. – 84 p.
10. CrowdStrike. *Global Threat Report 2023*. – Sunnyvale: CrowdStrike, 2023. – 80 p.
11. Check Point Research. *Cyber Attack Trends: 2023 Mid–Year Report*. – Tel Aviv: Check Point, 2023. – 77 p.
12. European Union Agency for Cybersecurity (ENISA). *Threat Landscape 2022*. – Luxembourg: Publications Office of the European Union, 2022. – 198 p.
13. PwC. *Global Digital Trust Insights 2023*. – London: PricewaterhouseCoopers, 2023. – 98 p.
14. Cisco. *Annual Cybersecurity Report 2023*. – San Jose: Cisco Press, 2023. – 142 p.
15. Symantec. *Internet Security Threat Report 2022*. – Mountain View: Symantec Corporation, 2022. – 110 p.

16. Europol. Internet Organised Crime Threat Assessment (IOCTA) 2023. – The Hague: Europol, 2023. – 86 p.
17. IBM. *Cost of a Data Breach Report 2023*. – Armonk: IBM Security, 2023. – 87 p.
18. Verizon. *2023 Data Breach Investigations Report*. – New York: Verizon, 2023. – 124 p.
19. Microsoft Security Team. *Digital Defense Report 2022*. – Redmond: Microsoft, 2022. – 140 p.
20. Palo Alto Networks. *Unit 42 Threat Report 2023*. – Santa Clara: PAN, 2023. – 93 p.
21. Kuchuk H ., Matvieiev M.. MODELING THE PROCESS OF LOADING 3D MODELS IN A CLIENT APPLICATION. *Advanced Information Systems, 9(4)*, 2022. P. 11–16.
22. Semenov, S., Zhang, M., Mozhaiev, O., Kuchuk, N., Tiulieniev, S., Gnusov, Y., Mozhaiev, M., Strukov, V., Onishchenko, Y., & Kuchuk, H. (2023). Construction of a model of steganographic embedding of the UAV identifier into ADS-B data. *Eastern-European Journal of Enterprise Technologies, 5(4 (125)*, 2020. 6 с.
23. В. М. Рудницький, Н. В. Лада, Г. А. Кучук, Д. А. Підласий. Архітектура СЕТ-операцій і технології потокового шифрування. *Architecture of CET-operations and stream encryption technologies*, монографія, Черкаси : видавець Пономаренко Р.В, 2024. – 374 с.
24. Kopp, A., Orlovskyi, D., Kizilov, O., & Halatova, O. (2024). Research on error probability assessment in user personal data processing in gdprcompliant business process models. *Bulletin of National Technical University "KhPI". Series: System Analysis, Control and Information Technologies, 1 (11)*, 2020. – 34 с.
25. Kopp, A. M., & Orlovskyi, D. L. (2020). Capturing software requirements for business process model analysis and improvement. *Bulletin of National Technical University "KhPI". Series: System Analysis, Control and Information Technologies, 2 (4)*, 2020. – 23 с.
26. Kopp, A., & Orlovskyi, D. The approach and the software tool to calculate semantic quality measures of business process models. *Bulletin of National Technical*

University "KhPI". Series: System Analysis, Control and Information Technologies, 1 (7), 2022– 66 с.

27. О. В. Шматко, О. Є. Рагулін, П. О. Кравченко, П. В. Буслов Дослідження архітектурних рішень для побудови безпечної системи зберігання та передачі конфіденційних даних. *Том 2 № 80 Системи управління, навігації та зв'язку,*2025 – 217с.
28. Shmatko, O., Yevseiev, S., Dudykevych, V., Milevskyi, S., Solnyshkova, S., Havrylova, A., Shestak, Y., Oriekhov, S., Korsunov, S., & Kravchenko, S. *Development of a method for synthesizing an information-analytical system for assessing the level of information transmission channels protection. Eastern-European Journal of Enterprise Technologies, 29 (128)*, – 36 p.
29. Shmatko, O., Yevseiev, S., Dudykevych, V., Milevskyi, S., Solnyshkova, S., Havrylova, A., Shestak, Y., Oriekhov, S., Korsunov, S., & Kravchenko, S. *Development of a method for synthesizing an information-analytical system for assessing the level of information transmission channels protection. Eastern-European Journal of Enterprise Technologies, 2(9) (128)*, 2024. –36 p.
30. Shmatko, O., Yevseiev, S., Milov, O., Sporyshev, K., Opirskyy, I., Glukhov, S., Rudenko, Y., Nalyvaiko, A., Dakov, S., & Sampir, O. *Development of a model of the information and analytical system for making decisions on detecting failures of information transmission channels. Eastern-European Journal of Enterprise Technologies, 3(9 (129)*, 2024. –28 p.
31. Toliupa S., Buchyk S., Nakonechnyi V., Brailovskyi M., Shtanenko S. Design of security protection and management systems based on game theory. *CEUR Workshop Proceedings*. – 2023. 334p.
32. Наконечний В., Сайко В., Наритник Т. Метод підвищення ефективності керування енергетичним потенціалом захищених радіоліній терагерцового діапазону з використанням штучного інтелекту *Безпека інформаційних систем і технологій, № 1(6),*2023. – 43с.

33. Дудикевич В.Б., Партика О.О., Наконечний Т.І. Впровадження систем одноразового входу (SSO) для підвищення кібербезпеки. *Сучасний захист інформації.* Т. 1(61), 2025. –60 с.
34. Pevnev, V., Tsuranov, M., Zemlianko, H., Amelina, O. Conceptual Model of Information Security. In: Nechyporuk, M., Pavlikov, V., Kritskiy, D. (eds) *Integrated Computer Technologies in Mechanical Engineering, 2020. ICTM 2020. Lecture Notes in Networks and Systems, vol 188.* Springer, Cham, *2020.*
35. V. Pevnev, M. Tsuranov and A. Zhmyrov, Noise-immune encoding: The aspects of cybersecurity assurance, *IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT),* Kyiv, Ukraine, 2018. –248p.
36. Sharov V.O., Berdnikov A.G. Model of a noise-resistant data transmission channel. *Computer modeling in science-intensive technologies (KMNT-2020),* Kharkiv: V.N. Karazin Kharkiv National University, 2020. 4 p.
37. Sharov V.O., Berdnikov A.G. Modeling of corrective cascade code in data transmission channels of the control system. *Computer modeling in science-intensive technologies (KMNT-2021),* Kharkiv: V.N. Karazin Kharkiv National University, 2021. 5 p.
38. Sharov V.O., Nikulina O.M., Severyn V.P. Development of a model of noise-tolerant data transmission for information technology of optimization of dynamic systems control. *Bulletin of NTU "KhPI". Series: System analysis, management and information technologies, No. 2 (8),* 2022, pp. 57–62.
39. Sklar B. Digital Communications: Fundamentals and Applications. 3rd ed. – Pearson, 2021. – 944 p.
40. Lin S., Costello D.J. Error Control Coding. 3rd ed. – Boston: Pearson, 2021. – 1280 p.
41. Proakis J.G., Salehi M. Digital Communications. 6th ed. – New York: McGraw–Hill, 2019. – 1072 p.

42. Comparative benchmarks: various independent studies comparing WireGuard, OpenVPN and IPSec (academic and industry reports) – aggregated analysis, 2019–2023. (See examples: Phoronix tests, networking research papers).
43. Touch J., Fairhurst G., Eggert S. RFC 8900: *IP Fragmentation Considered Fragile* (BCP 230), 2020. Electronic source, URL: https://www.rfc-editor.org/rfc/rfc8900.pdf. (дата звернення 10.05.2025)
44. Shu Lin, Daniel J. Costello, Jr., Mitsuru U. Practical Applications of Error Control Coding in Communication Systems. – Wiley–IEEE Press, 2020. – 432 p.
45. ETSI. 5G; NR; Multiplexing and channel coding *(3GPP TS 38.212 version 17.3.0 Release 17). – Sophia Antipolis*: ETSI, 2022. – 146 p.
46. IETF RFC 6363. Adamson B. et al. Forward Error Correction (FEC) Framework. RFC Editor, 2011. – URL: https://datatracker.ietf.org/doc/html/rfc6363 (дата звернення: 16.10.2025).
47. Watson M. et al. RFC 6363: *Forward Error Correction (FEC) Framework*, 2011 – URL: https://www.rfc-editor.org/rfc/rfc6363.html (дата звернення: 16.10.2025).
48. Richardson T., Urbanke R. Modern Coding Theory. – Cambridge: Cambridge University Press, 2008. – 576 p.
49. IETF RFC 8680. Roca V., Teibi S. Forward Error Correction (FEC) Framework Extension to Sliding Encoding Window Codes. RFC Editor, 2020. – URL: https://www.rfc–editor.org/rfc/rfc8680.html (дата звернення: 16.10.2025).
50. Roca V., Teibi S. RFC 8680: FECFRAME Extension to Sliding Encoding Window Codes, 2020 – URL: https://www.rfc-editor.org/rfc/rfc8680.pdf (дата звернення: 17.11.2025).
51. NASA. Space Communications and Navigation (SCaN) Code Recommendations. – Washington: NASA, 2020. – 84 p.
52. 3GPP TS 38.212 *NR; Multiplexing and channel coding*. ETSI/3GPP, Release 16–18 URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3214 (дата звернення: 9.5.2025).

53. CCSDS 131.x–series / NASA SCaN: *LDPC Codes for Near–Earth and Deep–Space Links*, 2006–2024 – URL: https://ccsds.org/Pubs/131x1o1s.pdf (дата звернення: 2.5.2025).
54. Cloudflare Research. Post–Quantum Cryptography and VPN Tunneling. – Cloudflare, 2022. – URL: https://www.rfc–editor.org/rfc/rfc8680.html (дата звернення: 16.10.2025).
55. Google Security Blog. Experimenting with Post–Quantum VPN. – Google LLC, 2026. – URL: https://blog.google/innovation-and-ai/technology/safety-security/the-quantum-era-is-coming-are-we-ready-to-secure-it/ (дата звернення: 7.2.2026).
56. ITU–T Recommendation X.200. Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model. – Geneva: ITU, 2016. – 138 p.
57. Saxena M. C., Bajaj P., et al. A Novel Method to Enhance the Reliability of Transmission over Secured SD–WAN Overlays (Reed–Solomon FEC + WireGuard). JATIT, 2023. – URL: https://www.jatit.org/volumes/Vol101No14/7Vol101No14.pdf (дата звернення: 16.10.2025).
58. Jones T., Fairhurst G., Tüxen T. RFC 8899: *Datagram PLPMTUD*, 2020 – URL: https://www.rfc-editor.org/rfc/rfc8899.pdf (дата звернення: 6.6.2024).
59. ENISA. Quantum–Safe Cryptography: Current State and Roadmap 2022–2035. – Luxembourg: *Publications Office of the EU*, 2022. – 88 p.
60. Sharov V.O., Nikulina O.M., Severyn V.P. Modeling and analysis of noise-resistant cascade code encoders for dynamic systems. *Bulletin of NTU "KhPI". Series: System analysis, management and information technologies, No. 1 (9)*, 2023, pp. 64–69.
61. Sharov V.O., Nikulina O.M., Loshkareva S.E. Development of a flexible model of noise-resistant data transmission for controlling dynamic systems. Information technologies: science, engineering, technology, education, health: *Abstracts of the XXI international scientific and practical conference MicroCAD-2023, May 17-20*, 2023, Kharkiv, NTU "KhPI", p. 1048.

62. Sharov V.O., Nikulina O.M. Two-level concept for modeling a single noise-resistant digital data transmission. *Bulletin of NTU "KhPI". Series: System Analysis, Management and Information Technologies, No. 1 (11)*, 2024, pp. 70–75.
63. Donenfeld J. WireGuard: Next Generation Kernel Network Tunnel. *Whitepaper & project documentation*. 2017–2020.
64. OpenVPN Community Documentation. OpenVPN Features and Comparisons. – OpenVPN.net. 2023.
65. Wouters P., Migault D., Mattsson J. P., Nir Y., Kivinen T. Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH*). RFC 8221. IETF / RFC Editor*, 2017.
66. Bruce Schneier, Mudge, Wagner D. Cryptanalysis of Microsoft's PPTP Authentication Extensions. – *Proceedings of USENIX Security Symposium*, 1999. – 12 p.
67. Kent S., Seo K. Security Architecture for the Internet Protocol. *RFC 4301. – IETF*, 2005. – 84 p.
68. Kaufman C., Hoffman P., Nir Y., Eronen P., Kivinen T. Internet Key Exchange Protocol Version 2 (IKEv2). *RFC 7296. – IETF*, 2014. – 142 p.
69. Schneier B. Secrets and Lies: Digital Security in a Networked World. – Wiley, 2015. – 448 p.
70. V2Ray / XRay project documentation and articles (project repos and community guides). 2015–2022.
71. Cisco Systems. SD–WAN and VPN Integration: Technical White Paper. – San Jose: Cisco, 2022. – 42 p.
72. ETSI. Network Functions Virtualisation and Cloud–native VPN. – Sophia Antipolis: ETSI, 2021. – 72 p.
73. Palo Alto Networks. SASE and the Future of Enterprise VPN. – Santa Clara: PAN, 2022. – 48 p.

74. Gartner. Market Guide for Virtual Private Networks. – Stamford: Gartner Inc., 2023. – 65 p.
75. IDC. Worldwide VPN Market Forecast, 2023–2030. – Framingham: IDC, 2023. – 54 p.
76. Forrester. Zero Trust and VPN Convergence. – Cambridge: Forrester Research, 2023. – 39 p.
77. Phoronix. Comparative Benchmarks of WireGuard, OpenVPN, IPSec and XRay. – Phoronix.com, 2023.
78. Mackey S., Mihov S., et al. A Performance Comparison of WireGuard and OpenVPN. ACM SAC'20, 2020.
79. Chua C.H., et al. Open–Source VPN Software: Performance Comparison, ACM (2022).
80. Anyam J., Singh R.R., Larijani H., Philip A. Empirical Performance Analysis of WireGuard vs. OpenVPN in Cloud and Virtualised Environments. MDPI Computers, 2025.
81. Dekker E. Performance Comparison of VPN Implementations: WireGuard, OpenVPN, IPsec. OS3 Report, 2020.
82. Sharov V.O., Nikulina O.M. Study of compatibility of methods and technologies of high-level protocols and error-correcting codes. *Bulletin of NTU "KhPI". Series: System analysis, management and information technologies, No. 2 (12),* 2024, pp. 92–97.
83. Sharov V.O., Nikulina O.M. Model of a noise-resistant control system taking into account artificial higher-level interference. *Information technologies: science, engineering, technology, education, health: Abstracts of the XXII international scientific and practical conference MicroCAD-2024*, May 22-24, 2024, Kharkiv, NTU "KhPI", p. 1270.
84. Sharov V.O., Nikulina O.M. The model control system resistant to interference from higher-level artificial sources. *XVIII International Scientific and Practical Conference of Masters and Postgraduates "Theoretical and Practical Research of*

Young Scientists”, November 19–22, 2024, Kharkiv: NTU “KhPI”, pp. 56–57.2024 р., Харків: НТУ «ХПІ», с. 56–57.

85. Sharov V.O., Nikulina O.M. Layered Defense in Communication Systems: Joint Use of VPN Protocols and Linear Block Codes. *Bulletin of NTU "KhPI". Series: System Analysis, Management and Information Technologies, No. 1 (13)*, 2025, pp. 112–116.

ДОДАТОК А
СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА

ШАРОВА Владислава Олеговича

Наукові праці, які відображають основні наукові результати дисертації.

Статті у періодичних наукових виданнях, що увійшли до переліку наукових фахових видань України:

1. Шаров В.О., Нікуліна О.М., Северин В.П. Розробка моделі завадостійкої передачі даних для інформаційної технології оптимізації управління динамічними системами. *Вісник НТУ «ХПІ». Серія: Системний аналіз, управління та інформаційні технології, № 2 (8)*, 2022, с. 57–62.(Б)

DOI: https://doi.org/10.20998/2079-0023.2022.02.09

2. Шаров В.О., Нікуліна О.М., Северин В.П. Моделювання та аналіз кодерів завадостійких каскадних кодів для динамічних систем. *Вісник НТУ «ХПІ». Серія: Системний аналіз, управління та інформаційні технології, № 1 (9)*, 2023, с. 64–69.(Б)

DOI: https://doi.org/10.20998/2079-0023.2023.01.10

3. Шаров В.О., Нікуліна О.М. Дворівнева концепція для моделювання єдиної завадостійкої передачі цифрових даних. *Вісник НТУ «ХПІ». Серія: Системний аналіз, управління та інформаційні технології, № 1 (11)*, 2024, с. 70–75.(Б)

DOI: https://doi.org/10.20998/2079-0023.2024.01.11

4. Sharov V.O., Nikulina O.M. Study of compatibility of methods and technologies of high-level protocols and error-correcting codes. *Вісник НТУ «ХПІ». Серія: Системний аналіз, управління та інформаційні технології, № 2 (12)*, 2024, с. 92–97.(Б)

DOI: https://doi.org/10.20998/2079-0023.2024.02.14

5. Sharov V.O., Nikulina O.M. Layered Defense in Communication Systems: Joint Use of VPN Protocols and Linear Block Codes. *Вісник НТУ «ХПІ». Серія: Системний аналіз, управління та інформаційні технології, № 1 (13)*, 2025, с. 112–116.(Б)

DOI: https://doi.org/10.20998/2079-0023.2025.01.17

Інші публікації:

Опубліковані праці апробаційного характеру:

6. Шаров В.О. Модель завадостійкого каналу передачі даних / Шаров В.О., Бердніков А.Г.// *Комп'ютерне моделювання в наукоємних технологіях (КМНТ-2020)*, Харків: ХНУ ім. В.Н. Каразіна, 2020. 4 с.

URL: https://discovery.kpi.ua/Record/000634216

7. Шаров В.О. Моделювання коригувального каскадного коду в каналах передачі даних системи управління / Шаров В.О., Бердніков А.Г.// *Комп'ютерне моделювання в наукоємних технологіях (КМНТ-2021)*, Харків: ХНУ ім. В.Н. Каразіна, 2021. 5 с.

URL: https://odnb.odessa.ua/vnn/book/13913

8. Шаров В.О. Розробка гнучкої моделі завадостійкої передачі даних для управління динамічними системами / Шаров В.О., Нікуліна О.М., Лошкарьова С.Є.// *Інформаційні технології: наука, техніка, технологія, освіта, здоров'я:* Тези доповідей XXXI міжнародної науково-практичної конференції MicroCAD-2023, 17-20 травня 2023 р., Харків, НТУ «ХПІ», с. 1048.

URL: https://repository.kpi.kharkov.ua/items/ea5b83c5-0561-47cb-a4d0-67aacd51c994

9. Шаров В.О. Модель завадостійкої системи управління з урахуванням штучних перешкод вищого рівня / Шаров В.О., Нікуліна О.М. // *Інформаційні технології: наука, техніка, технологія, освіта, здоров'я:* Тези доповідей XXXII міжнародної науково-практичної конференції MicroCAD-2024, 22-24 травня 2024 р., Харків, НТУ «ХПІ», с. 1270.

URL: https://repository.kpi.kharkov.ua/server/api/core/bitstreams/6c1dd37f-bc26-4c91-af1c-a7eec5d2d9b5

10. Sharov V.O. The model control system resistant to interference from higher-level artificial sources. / Sharov V.O., Nikulina O.M. // XVIII Міжнар. наук.-практ. конф. магістрантів та аспірантів «Теоретичні та практичні дослідження молодих вчених», 19–22 листопада 2024 р., Харків: НТУ «ХПІ», с. 56–57.

URL: https://repository.kpi.kharkov.ua/items/78bb4ab5-ac4b-4c40-aa1f-6ff555b2823f