

## Кібербезпека

Галузі знань: 12 «Інформаційні технології», спеціальність: 125 «Кібербезпека», кваліфікація: доктор філософії з кібербезпеки

№	Прізвище, ім'я по батькові аспіранта (рік вступу, тема дисертації)	Прізвище, ім'я по батькові наукового керівника	Відповідність напрямку досліджень
1	Подгайко Владислав Олегович, 2020, "Моделі та методи використання біометричних ознак в системах електронних довірчих послуг"	Рассомахін Сергій Геннадійович	<b>П1 - Публ. наукового керівника</b> 1. Modulation in electronics and Telecommunications / Intech Open . London, 2020. Print ISBN 978-1-78985-489-3, Online ISBN 978-1-78985-490-9, eBook(PDF) ISBN 978-1-83968-965-9. 2. Security and noise immunity of telecommunication systems: new solutions to the codes and signals design problem. Collective monograph. edited by Sergey G. Rassomakhin and Alexander A. Kuznetsov. ASC Academic Publishing. 2017.– 198 p.– ISBN:978-0-9989826-2-5 (Hardback), ISBN:978-0-9989826-3-2 (Ebook). 3. Rassomakhin, S.G. Mathematical and physical nature of the channel capacity. Telecommunications and Radio Engineering, 2017, 76(16), p. 1423-1451. 4. Rassomakhin, S., Serbin, V., Kuznetsova, T. Method for recognizing and processing complex signals. 2019CEUR Workshop Proceedings 2353, p. 71-84. 5. Rassomakhin, S., Budianska, K., Bagmut, M. Mathematical model of the biometric system of fingerprint authentication for modern web-services. 2019, CEUR Workshop Proceedings 2588. 6. Rassomakhin, S. Lavrovska, T., The method of pseudorandom codes decoding on the basis of the modified method of branches and boundaries. 2017 4th International Scientific-Practical Conference Problems of Infocommunications Science and Technology, PIC S and T. Proceedings 2018-January, p. 305-310. 7. Рассомахин С. Г., Т. В. Лавровская Математические модели случайных и псевдослучайных кодов // Системы обработки информации. - 2016. - № 9. - С. 55-61.

			<p>8. Рассомахин С. Г., Веклич С. Г. Линейная алгебраическая обработка сложных сигнальных конструкций // Системы обработки информации. - 2016. - № 8. — С. 40-43.</p> <p>9. Рассомахин С.Г., Лавровская Т.В. Математический метод декодирования псевдослучайных кодов на основе модифицированного метода ветвей и границ // Системы управления, навигации та зв'язку. – П. : Полтавський національний технічний університет імені Юрія Кондратюка, 2016. – Вип. 3 (39). – С. 42 – 56.</p> <p>10. Мелкозьорова О.М., Рассомахин С.Г. Ідентифікація відбитків пальців на основі Гамільтонових циклів розподілу локальних ознак. Вісник Харківського національного університету імені В.Н. Каразіна, серія «Математичне моделювання. Інформаційні технології. Автоматизовані системи управління», 2020. том 44, с. 51-65.</p> <p><b>П2 - Публ. аспіранта</b></p> <p>1. Акользіна О.С., Бобух В.А., Подгайко В.О. Аналіз стійкості NTRU Prime, як кандидата на постквантовий алгоритм направленої шифрування.// Збірка праць V Міжнар. наук.-техн. конференції «Комп'ютерне моделювання в наукоємних технологіях». – Харків, 2018. – С. 24-28.</p> <p>2. Подгайко В.О., Акользіна О.С. Аналіз алгоритму Streamlined NTRU Prime, як кандидата на роль постквантового алгоритму направленої шифрування. // Збірник матеріалів VIII Міжнар. наук.-техн. конференції «Захист інформації і безпека інформаційних систем». – Львів, 2019. . – С. 1-2.</p> <p>3. Подгайко В.О., Акользіна О.С. Порівняння кандидатів КЕМ на пост квантовий стандарт NIST на основі експертних оцінок із застосуванням методу вагових коефіцієнтів. // Збірник матеріалів XI наук.-практичної конференції «Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення. Застосування підрозділів, комплексів, засобів зв'язку та автоматизації в операції Об'єднаних сил». – Київ, 2018. . – С. 1-5.</p>
--	--	--	--

			<p>4. Подгайко В.О., Мельник Т.В. Схема цифрового підпису NTRU Prime, стійкого до атак на квантових комп'ютерах. // Матеріали VI Міжнар. наук.-техн. конференції «Захист інформації і безпека інформаційних систем». – Львів, 2017. – С. 1-2</p> <p>5. Акользіна О.С., Подгайко В.О. Аналіз актуальних досліджень щодо криптографії на решітках. // Журнал: Математичне та комп'ютерне моделювання: Серія технічні науки. – Кам'янець-Подільськ: Кам'янець-Подільський НУ ім. Івана Огієнка, 2019. – С. 20-25.</p> <p>6. Акользіна О.С., Подгайко В.О. Аналіз актуальних проблемних питань щодо перспективної асиметричної криптографії. // Журнал: Математичне та комп'ютерне моделювання: Серія технічні науки. – Кам'янець-Подільськ: Кам'янець-Подільський НУ ім. Івана Огієнка, 2019. – С. 3-10.</p> <p>7. Yurii Gorbenko; Olha Akolzina; Vladyslav Podhaiko. Modern attacks analysis for NTRU-similar algorithms. // Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&amp;T), 2017 4th International, Kharkiv, Ukraine, 2017 [SCOPUS] IEEE: веб-сайт. URL: <a href="https://ieeexplore.ieee.org/document/8246411">https://ieeexplore.ieee.org/document/8246411</a> (дата звернення 05.09.19).</p>
2	Каптьол Євген Юрійович, 2020, "Методи оцінки та порівняльного аналізу симетричних електронних підписів стійких до класичного та квантового криптоаналізу"	Горбенко Іван Дмитрович	<p><b>ПІ - Публ. наукового керівника</b></p> <p>1. Gorbenko, I.D., Kachko, O.G., Yesina, M.V., 2018. Analysis of asymmetric NTRU Prime IT Ukraine encryption algorithm with regards to known attacks. Telecommunications and Radio Engineering, vol. 77. <a href="https://doi.org/10.1615/TelecomRadEng.v77.i9.50">https://doi.org/10.1615/TelecomRadEng.v77.i9.50</a></p> <p>2. Gorbenko, Y.I., Melnik, T.V., Gorbenko, I.D., 2018. Analysis of potential post-quantum schemes of hash-based digital signature. Telecommunications and Radio Engineering, vol. 77. <a href="https://doi.org/10.1615/TelecomRadEng.v77.i7.40">https://doi.org/10.1615/TelecomRadEng.v77.i7.40</a></p> <p>3. Gorbenko, I.D., Alekseychuk, A.N., Kachko, O.G., Yesina, M.V., Stelnik, I.V., Kandy, S.O., Bobukh, V.A., Ponomar, V.A., 2019a. Calculation of general parameters for NTRU Prime Ukraine of 6-7 levels of stability. Telecommunications and Radio Engineering, vol. 78. <a href="https://doi.org/10.1615/TelecomRadEng.v78.i4.40">https://doi.org/10.1615/TelecomRadEng.v78.i4.40</a></p>

			<p>4. Gorbenko, I.D., Kachko, O.G., Gorbenko, Y.I., Stelnik, I.V., Kandy, S.O., Yesina, M.V., 2019b. Methods of building general parameters and keys for NTRU Prime Ukraine of 5th – 7th levels of stability. Product form. Telecommunications and Radio Engineering, vol. 78. <a href="https://doi.org/10.1615/TelecomRadEng.v78.i7.30">https://doi.org/10.1615/TelecomRadEng.v78.i7.30</a></p> <p>5. Gorbenko, I., Kachko, O., Akolzina, o, 2018a. Research of post-quantum public key encryption algorithm, in: 2018 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo). Presented at the 2018 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo), pp. 1–4. <a href="https://doi.org/10.1109/UkrMiCo43733.2018.9047585">https://doi.org/10.1109/UkrMiCo43733.2018.9047585</a></p> <p>6. Gorbenko, I., Kachko, O., Yesina, M., Akolzina, O., 2018b. Post-quantum algorithm of asymmetric encryption and its basic properties, in: 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT). Presented at the 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (Dessert), pp. 265–270. <a href="https://doi.org/10.1109/dessert.2018.8409142">https://doi.org/10.1109/dessert.2018.8409142</a></p> <p>7. Gorbenko, I., Kudryashov, I., Malieieva, H., 2018c. Comparative Analysis of Candidates for a Post-Quantum CPU Based on MQ Cryptographic Transformation, in: 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S T). Presented at the 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC ST), pp. 442–446. <a href="https://doi.org/10.1109/infocommst.2018.8632070">https://doi.org/10.1109/infocommst.2018.8632070</a></p> <p>8. Gorbenko I. Proposals of comparative analysis and decision making during the competition regarding the certain benefits of asymmetric post quantum cryptographic primitives / I. Gorbenko, Yu. Gorbenko, M. Yesina, V. Ponomar // Computer Science And Cybersecurity. – V. N. Karazin Kharkiv National University, 2017, Issue 1(5) – P. 53–70. Access mode: <a href="http://periodicals.karazin.ua/cscs/article/view/8307">http://periodicals.karazin.ua/cscs/article/view/8307</a>.</p> <p>9. Gorbenko I. Research of usage possibility and post-quantum algorithms advantages depend on application conditions / I. Gorbenko,</p>
--	--	--	---

			<p>Yu. Gorbenko, V. Ponomar, M. Yesina // Computer Science And Cybersecurity. – V. N. Karazin Kharkiv National University, 2017, Issue 3(7) – P. 45–66. Access mode: <a href="http://periodicals.karazin.ua/cscs/article/view/10005/9528">http://periodicals.karazin.ua/cscs/article/view/10005/9528</a>.</p> <p>11. Gorbenko I. D. NTRU Prime IIT Ukraine encryption algorithm with consideration known attacks analysis / I. D. Gorbenko, O.G. Kachko, M. V. Yesina // Computer Science And Cybersecurity. – V. N. Karazin Kharkiv National University, 2017, Issue 4(8) – P. 4–16. Access mode: <a href="https://periodicals.karazin.ua/cscs/article/view/10452/10192">https://periodicals.karazin.ua/cscs/article/view/10452/10192</a>.</p> <p>12. Gorbenko I. D. General statements and analysis of the end-to-end encryption algorithm NRTU Prime IIT Ukraine / I. D. Gorbenko, O. G. Kachko, M. V. Yesina // Radiotechnika. – Kh. : Kharkiv National University of Radio Electronics, 2018. – Issue 193 – P. 5–16.</p> <p>13. Gorbenko Ivan The problem of cryptographic transformations standardization and the state of its solution / Ivan Gorbenko, Olena Kachko, Oleksandr Kuznetsov, Yurii Gorbenko, Maryna Yesina // VII International Scientific and Technical Conference “ Information protection and security of information systems ” : Proceedings of the Scientific and Technical Conference, 30–31 May 2019. – L. : Lviv Polytechnic National University, 2019. – P. 84-85.</p> <p>14. Yesina Maryna Research of security models of post-quantum cryptographic primitives / Maryna Yesina // VII International Scientific and Technical Conference “ Information protection and security of information systems ” : Proceedings of the Scientific and Technical Conference, 30–31 May 2019. – L. : Lviv Polytechnic National University, 2019. – P. 118-119.</p> <p>15. Yesina Maryna Comparative Analysis of Key Encapsulation Mechanisms / Maryna Yesina, Mikolaj Karpinski, Volodymyr Ponomar, Yuriy Gorbenko, Tomasz Gancarczyk, Uliana Iatsykovska // Proceedings of the 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS). September 18-21, 2019, Metz, France. – Volume 1. – P. 7-12.</p> <p>16. Сутність та особливості реалізації методу Гровера на класичному комп'ютері для симетричного криптоаналізу / Ю. І.</p>
--	--	--	---

			<p>Горбенко, Є. Ю. Каптьол // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2018. Вип. 195. – С. 89-100. DOI: <a href="https://doi.org/10.30837/rt.2018.4.195.09">https://doi.org/10.30837/rt.2018.4.195.09</a>.</p> <p>17. Аналіз стійкості криптографічних примітивів на основі метода Гровера / Каптьол Є. Ю., Горбенко І. Д. // Комп'ютерне Моделювання В Наукоємних Технологіях: Праці Міжнародної Науково-Технічної Конференції. Харків – 2018. С. 129-132.</p> <p>18. Grover's method essential and software model for symmetric cryptanalysis / Yevhenii Kaptol, Ivan Gorbenko // Захист Інформації І Безпека Інформаційних Систем: Матеріали VII міжнародної науково-технічної конференції. Львів – 2019. С. 37-48. DOI: <a href="https://doi.org/10.30837/rt.2020.3.202.03">https://doi.org/10.30837/rt.2020.3.202.03</a></p> <p>19. Аналіз можливостей та особливості програмування задач криптології на квантовому комп'ютері / Є. Ю. Каптьол, І. Д. Горбенко // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2020. Вип. 202. – С. 89-100.</p> <p>20. Аналіз можливостей та особливості програмування на квантовому комп'ютері / Каптьол Є.Ю., Горбенко І.Д. // XIII науково-практична конференція «Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення. Застосування підрозділів, комплексів, засобів зв'язку, автоматизації та кібербезпеки в операції Об'єднаних сил» (Доповіді та тези доповідей). Київ – 2020. С. 49-55</p> <p><b>П2 - Публ. аспіранта</b></p> <p>1. Сутність та особливості реалізації методу Гровера на класичному комп'ютері для симетричного криптоаналізу / Ю. І. Горбенко, Є. Ю. Каптьол // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2018. Вип. 195. – С. 89-100. URL: <a href="https://doi.org/10.30837/rt.2018.4.195.09">https://doi.org/10.30837/rt.2018.4.195.09</a> (Google Scholar, ICI World of Journals, Національна бібліотека України імені В. І. Вернадського)</p> <p>2. Аналіз стійкості криптографічних примітивів на основі метода Гровера / Каптьол Є. Ю., Горбенко І. Д. // Комп'ютерне</p>
--	--	--	---

			<p>моделивання в наукоємних технологіях: Праці міжнародної науково-технічної конференції. Харків – 2018. С. 129-132.</p> <p>3. Grover’s method essential and software model for symmetric cryptanalysis / Yevhenii Kaptol, Ivan Gorbenko // ЗАХИСТ ІНФОРМАЦІЇ І БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ: МАТЕРІАЛИ VII міжнародної науково-технічної конференції. Львів – 2019. С. 37-48. URL: <a href="https://doi.org/10.30837/rt.2020.3.202.03">https://doi.org/10.30837/rt.2020.3.202.03</a></p> <p>4. Аналіз можливостей та особливості програмування задач криптології на квантовому комп’ютері / Є. Ю. Каптьол, І. Д. Горбенко // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2020. Вип. 202. – С. 89-100. (Google Scholar, ICI World of Journals, Національна бібліотека України імені В. І. Вернадського)</p> <p>5. Аналіз можливостей та особливості програмування на квантовому комп’ютері / Каптьол Є.Ю., Горбенко І.Д. // XIII науково-практична конференція «Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення. Застосування підрозділів, комплексів, засобів зв’язку, автоматизації та кібербезпеки в операції Об’єднаних сил» (Доповіді та тези доповідей). Київ – 2020. С. 49-55.</p>
3	Курбатов Олександр Сергійович, 2020 "Моделі та методи побудови протоколів електронного голосування для підвищення анонімності голосуючих, а також відмовостійкості та цензуростійкості системи"	Кузнецов Олександр Олександрович	<p><b>III - Публ. наукового керівника</b></p> <p>1. Gorbenko, I., Kuznetsov, A., Lutsenko, M., Ivanenko, D., 2017. The research of modern stream ciphers, in: 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S T). Presented at the 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S T), pp. 207–210. <a href="https://doi.org/10.1109/INFOCOMMST.2017.8246381">https://doi.org/10.1109/INFOCOMMST.2017.8246381</a></p> <p>2. Gorbenko, I., Kuznetsov, A., Tymchenko, V., Gorbenko, Y., Kachko, O., 2018a. Experimental Studies Of The Modern Symmetric Stream Ciphers, in: 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S T). Presented at the 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S T), pp. 125–128. <a href="https://doi.org/10.1109/INFOCOMMST.2018.8632058">https://doi.org/10.1109/INFOCOMMST.2018.8632058</a></p>

			<p>3. Gorbenko, I., Kuznetsov, A., Tymchenko, V., Gorbenko, Y., Kachko, O., 2018a. Experimental Studies Of The Modern Symmetric Stream Ciphers, in: 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S T). Presented at the 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S T), pp. 125–128. <a href="https://doi.org/10.1109/INFOCOMMST.2018.8632058">https://doi.org/10.1109/INFOCOMMST.2018.8632058</a></p> <p>4. Kuznetsov, A., Frolenko, V., Eremin, E., Zavgorodnia, O., 2018a. Research of cross-platform stream symmetric ciphers implementation, in: 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT). Presented at the 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), pp. 300–305. <a href="https://doi.org/10.1109/DESSERT.2018.8409148">https://doi.org/10.1109/DESSERT.2018.8409148</a></p> <p>5. Kuznetsov, A., Kiian, A., Gorbenko, Y., Smirnov, O., Cherep, O., Bexhter, L., 2019c. Code-based Pseudorandom Generator for the Post-Quantum Period, in: 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT). Presented at the 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT), pp. 204–209. <a href="https://doi.org/10.1109/ATIT49449.2019.9030493">https://doi.org/10.1109/ATIT49449.2019.9030493</a></p> <p>6. Kuznetsov, A., Lutsenko, M., Kuznetsova, K., Martyniuk, O., Babenko, V., Perevozova, I., 2019i. Statistical Testing of Blockchain Hash Algorithms, in: Fedushko, S., Gnatyuk, S., Peleshchyshyn, A., Hu, Z., Odarchenko, R., Korobiichuk, I. (Eds.), Proceedings of the International Workshop on Conflict Management in Global Information Networks (CMiGIN 2019) Co-Located with 1st International Conference on Cyber Hygiene and Conflict Management in Global Information Networks (CyberConf 2019), Lviv, Ukraine, November 29, 2019, CEUR Workshop Proceedings. CEUR-WS.org, pp. 67–79.</p> <p>7. Rassomakhin, S., Kuznetsov, A., Shlokin, V., Belozertsev, I., Serhiienko, R., 2018. Mathematical Model for the Probabilistic Minutia Distribution in Biometric Fingerprint Images, in: 2018 IEEE Second International Conference on Data Stream Mining Processing (DSMP). Presented at the 2018 IEEE Second International Conference on Data</p>
--	--	--	--



			<p>Stream Mining Processing (DSMP), pp. 514–518. <a href="https://doi.org/10.1109/DSMP.2018.8478496">https://doi.org/10.1109/DSMP.2018.8478496</a></p> <p>8. Shapoval, O., Kuznetsov, A., Poluyanenko, N., Yakovenko, V., Prokopovych-Tkachenko, D., Kavun, S., 2019. The Decentralized Voting Model Using the Hyperledger Platform Paper, in: 2019 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo). Presented at the 2019 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo), pp. 1–5. <a href="https://doi.org/10.1109/UkrMiCo47782.2019.9165368">https://doi.org/10.1109/UkrMiCo47782.2019.9165368</a></p> <p>9. Shekhanin, K., Kuznetsov, A., Krasnobayev, V., Smirnov, O., 2020. Detecting Hidden Information in FAT. IJCNIS 12, 33–43. <a href="https://doi.org/10.5815/ijcnis.2020.03.04">https://doi.org/10.5815/ijcnis.2020.03.04</a></p> <p>10. Shekhanin, K.Y., Kolhatin, A.O., Demenko, E.E., Kuznetsov, A.A., 2019. On Hiding Data Into The Structure Of The Fat Family File System. Tre 78. <a href="https://doi.org/10.1615/TelecomRadEng.v78.i11.50">https://doi.org/10.1615/TelecomRadEng.v78.i11.50</a></p> <p>11. Kuznetsov, O.O., Gorbenko, Y.I., Bilozertsev, I.M., Andrushkevych, A.V., Narizhnyi, O.P., 2018. ALGEBRAIC IMMUNITY OF NON-LINEAR BLOCKS OF SYMMETRIC CIPHERS. TRE 77. <a href="https://doi.org/10.1615/TelecomRadEng.v77.i4.30">https://doi.org/10.1615/TelecomRadEng.v77.i4.30</a></p> <p>12. Poluyanenko, N., Kuznetsov, A., Lazareva, E., Marakushyn, A., 2020. Extrapolation to calculate the probability of a double spending attack, in: Subbotin, S. (Ed.), Proceedings of The Third International Workshop on Computer Modeling and Intelligent Systems (CMIS-2020), Zaporizhzhia, Ukraine, April 27-May 1, 2020, CEUR Workshop Proceedings. CEUR-WS.org, pp. 610–620.</p> <p>13. Poluyanenko, N., Kuznetsov, A., Lisickiy, K., Datsenko, S., Nakisko, O., Rudenko, S., 2021. The Problem of Double Costs in Blockchain Systems, in: Hu, Z., Petoukhov, S., Dychka, I., He, M. (Eds.), Advances in Computer Science for Engineering and Education III, Advances in Intelligent Systems and Computing. Springer International Publishing, Cham, pp. 640–652. <a href="https://doi.org/10.1007/978-3-030-55506-1_57">https://doi.org/10.1007/978-3-030-55506-1_57</a></p> <p><b>П2 - Публ. аспіранта</b></p>
--	--	--	--

			<ol style="list-style-type: none"> <li>1. Global digital identity and public key infrastructure Kurbatov, O., Kravchenko, P., Poluyanenko, N., Demenko, Y., Kuznetsova, T. CEUR Workshop Proceedings, 2020, 2732, pp. 1–12</li> <li>2. Using Ring Signatures for An Anonymous E-Voting System Kurbatov, O., Kravchenko, P., Poluyanenko, N., Shapoval, O., Kuznetsova, T. 2019 IEEE International Conference on Advanced Trends in Information Theory, ATIT 2019 - Proceedings, 2019, pp. 187–190, 9030447</li> <li>3. Decentralized identification and certification system Kurbatov, O., Shapoval, O., Poluyanenko, N., Kuznetsova, T., Kravchenko, P. 2019 IEEE International Scientific-Practical Conference: Problems of Infocommunications Science and Technology, PIC S and T 2019 - Proceedings, 2019, pp. 507–510, 9061351</li> <li>4. Anonymous decentralized e-voting system Kurbatov, O., Kravchenko, P., Shapoval, O., Sakun, A., Kovtun, V. CEUR Workshop Proceedings, 2019, 2588</li> </ol>
4	Багмут Михайло Олександрович, 2019, "Моделі і методи біометричної автентифікації на основі відбитків пальців"	Рассомахін Сергій Геннадійович	<p><b>П1 - Публ. наукового керівника</b></p> <ol style="list-style-type: none"> <li>1. Modulation in electronics and Telecommunications / Intech Open . London, 2020. Print ISBN 978-1-78985-489-3, Online ISBN 978-1-78985-490-9, eBook(PDF) ISBN 978-1-83968-965-9.</li> <li>2. Security and noise immunity of telecommunication systems: new solutions to the codes and signals design problem. Collective monograph. edited by Sergey G. Rassomakhin and Alexander A. Kuznetsov. ASC Academic Publishing. 2017.– 198 p.– ISBN:978-0-9989826-2-5 (Hardback), ISBN:978-0-9989826-3-2 (Ebook).</li> <li>3. Rassomakhin, S.G. Mathematical and physical nature of the channel capacity. Telecommunications and Radio Engineering, 2017, 76(16), p. 1423-1451.</li> <li>4. Rassomakhin, S., Serbin, V., Kuznetsova, T. Method for recognizing and processing complex signals. 2019CEUR Workshop Proceedings 2353, p. 71-84.</li> <li>5. Rassomakhin, S., Budianska, K., Bagmut, M. Mathematical model of the biometric system of fingerprint authentication for modern web-services. 2019, CEUR Workshop Proceedings 2588.</li> </ol>

			<p>6. Rassomakhin, S. Lavrovska, T., The method of pseudorandom codes decoding on the basis of the modified method of branches and boundaries. 2017 4th International Scientific-Practical Conference Problems of Infocommunications Science and Technology, PIC S and T. Proceedings 2018-January, p. 305-310.</p> <p>7. Рассомахин С. Г., Т. В. Лавровская Математические модели случайных и псевдослучайных кодов // Системи обробки інформації. - 2016. - № 9. - С. 55-61.</p> <p>8. Рассомахин С. Г., Веклич С. Г. Линейная алгебраическая обработка сложных сигнальных конструкций // Системи обробки інформації. - 2016. - № 8. — С. 40-43.</p> <p>9. Рассомахин С.Г., Лавровская Т.В. Математический метод декодирования псевдослучайных кодов на основе модифицированного метода ветвей и границ // Системи управління, навігації та зв'язку. – П. : Полтавський національний технічний університет імені Юрія Кондратюка, 2016. – Вип. 3 (39). – С. 42 – 56.</p> <p>10. Мелкозьорова О.М., Рассомахин С.Г. Ідентифікація відбитків пальців на основі Гамільтонових циклів розподілу локальних ознак. Вісник Харківського національного університету імені В.Н. Каразіна, серія «Математичне моделювання. Інформаційні технології. Автоматизовані системи управління», 2020. том 44, с. 51-65.</p> <p><b>П2 - Публ. аспіранта</b></p> <p>1. Biometric authentication using convolutional neural networks Kuznetsov, A., Oleshko, I., Chernov, K., Bagmut, M., Smirnova, T. Lecture Notes in Networks and Systems, 2021, 152, стр. 85–98</p> <p>2. Biometric images attacks detecting using convolutional neural networks Chernov, K., Kuznetsova, K., Oleshko, I., Bagmut, M., Fedorchuk, A., Kryzhanovskyi, D. CEUR Workshop Proceedings, 2020, 2654, стр. 107–121</p> <p>3. Mathematical model of the biometric system of fingerprint authentication for modern web-services Rassomakhin, S., Budianska,</p>
--	--	--	---

			<p>K., Bagmut, M., ...Ivko, T., Kuznetsova, T. CEUR Workshop Proceedings, 2019, 2588</p> <p>4. Kuznetsov, A., Hryhorenko, V., Diachenko, A., &amp; Bagmut, M. (2019). Дисперсійний аналіз мережевого трафіку для виявлення вторгнень в Smart Grids. Комп'ютерні науки та кібербезпека, (1), 62-74. <a href="https://doi.org/10.26565/2519-2310-2019-1-06">https://doi.org/10.26565/2519-2310-2019-1-06</a></p> <p>5. Тезиси: XI-а Міжнародна науково-практична конференція «Free And Open Source Software» . Реалізація циліндр-кодів минутиць по отпечаткам пальцев. Багмут М.А., 2019.</p>
5	Луценко Марія Сергіївна, 2019, "Моделі та методи криптографічних перетворень з відкритим ключем із застосуванням алгебраїчних кодів"	Кузнецов Олександр Олександрович	<p><b>ПІ - Публ. наукового керівника</b></p> <p>1. Gorbenko, I., Kuznetsov, A., Lutsenko, M., Ivanenko, D., 2017. The research of modern stream ciphers, in: 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S T). Presented at the 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S T), pp. 207–210. <a href="https://doi.org/10.1109/INFOCOMMST.2017.8246381">https://doi.org/10.1109/INFOCOMMST.2017.8246381</a></p> <p>2. Gorbenko, I., Kuznetsov, A., Tymchenko, V., Gorbenko, Y., Kachko, O., 2018a. Experimental Studies Of The Modern Symmetric Stream Ciphers, in: 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S T). Presented at the 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S T), pp. 125–128. <a href="https://doi.org/10.1109/INFOCOMMST.2018.8632058">https://doi.org/10.1109/INFOCOMMST.2018.8632058</a></p> <p>3. Gorbenko, I., Kuznetsov, A., Tymchenko, V., Gorbenko, Y., Kachko, O., 2018a. Experimental Studies Of The Modern Symmetric Stream Ciphers, in: 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S T). Presented at the 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S T), pp. 125–128. <a href="https://doi.org/10.1109/INFOCOMMST.2018.8632058">https://doi.org/10.1109/INFOCOMMST.2018.8632058</a></p> <p>4. Kuznetsov, A., Frolenko, V., Eremin, E., Zavgorodnia, O., 2018a. Research of cross-platform stream symmetric ciphers implementation, in: 2018 IEEE 9th International Conference on Dependable Systems,</p>

			<p>Services and Technologies (DESSERT). Presented at the 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), pp. 300–305. <a href="https://doi.org/10.1109/DESSERT.2018.8409148">https://doi.org/10.1109/DESSERT.2018.8409148</a></p> <p>5. Kuznetsov, A., Kiian, A., Gorbenko, Y., Smirnov, O., Cherep, O., Bexhter, L., 2019c. Code-based Pseudorandom Generator for the Post-Quantum Period, in: 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT). Presented at the 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT), pp. 204–209. <a href="https://doi.org/10.1109/ATIT49449.2019.9030493">https://doi.org/10.1109/ATIT49449.2019.9030493</a></p> <p>6. Kuznetsov, A., Lutsenko, M., Kuznetsova, K., Martyniuk, O., Babenko, V., Perevozova, I., 2019i. Statistical Testing of Blockchain Hash Algorithms, in: Fedushko, S., Gnatyuk, S., Peleshchyshyn, A., Hu, Z., Odarchenko, R., Korobiichuk, I. (Eds.), Proceedings of the International Workshop on Conflict Management in Global Information Networks (CMiGIN 2019) Co-Located with 1st International Conference on Cyber Hygiene and Conflict Management in Global Information Networks (CyberConf 2019), Lviv, Ukraine, November 29, 2019, CEUR Workshop Proceedings. CEUR-WS.org, pp. 67–79.</p> <p>7. Rassomakhin, S., Kuznetsov, A., Shlokin, V., Belozertsev, I., Serhiienko, R., 2018. Mathematical Model for the Probabilistic Minutia Distribution in Biometric Fingerprint Images, in: 2018 IEEE Second International Conference on Data Stream Mining Processing (DSMP). Presented at the 2018 IEEE Second International Conference on Data Stream Mining Processing (DSMP), pp. 514–518. <a href="https://doi.org/10.1109/DSMP.2018.8478496">https://doi.org/10.1109/DSMP.2018.8478496</a></p> <p>8. Shapoval, O., Kuznetsov, A., Poluyanenko, N., Yakovenko, V., Prokopovych-Tkachenko, D., Kavun, S., 2019. The Decentralized Voting Model Using the Hyperledger Platform Paper, in: 2019 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo). Presented at the 2019 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo), pp. 1–5. <a href="https://doi.org/10.1109/UkrMiCo47782.2019.9165368">https://doi.org/10.1109/UkrMiCo47782.2019.9165368</a></p>
--	--	--	--

			<p>9. Shekhanin, K., Kuznetsov, A., Krasnobayev, V., Smirnov, O., 2020. Detecting Hidden Information in FAT. IJCNIS 12, 33–43. <a href="https://doi.org/10.5815/ijenis.2020.03.04">https://doi.org/10.5815/ijenis.2020.03.04</a></p> <p>10. Shekhanin, K.Y., Kolhatin, A.O., Demenko, E.E., Kuznetsov, A.A., 2019. On Hiding Data Into The Structure Of The Fat Family File System. Tre 78. <a href="https://doi.org/10.1615/TelecomRadEng.v78.i11.50">https://doi.org/10.1615/TelecomRadEng.v78.i11.50</a></p> <p>11. Kuznetsov, O.O., Gorbenko, Y.I., Bilozertsev, I.M., Andrushkevych, A.V., Narizhnyi, O.P., 2018. ALGEBRAIC IMMUNITY OF NON-LINEAR BLOCKS OF SYMMETRIC CIPHERS. TRE 77. <a href="https://doi.org/10.1615/TelecomRadEng.v77.i4.30">https://doi.org/10.1615/TelecomRadEng.v77.i4.30</a></p> <p>12. Poluyanenko, N., Kuznetsov, A., Lazareva, E., Marakushyn, A., 2020. Extrapolation to calculate the probability of a double spending attack, in: Subbotin, S. (Ed.), Proceedings of The Third International Workshop on Computer Modeling and Intelligent Systems (CMIS-2020), Zaporizhzhia, Ukraine, April 27-May 1, 2020, CEUR Workshop Proceedings. CEUR-WS.org, pp. 610–620.</p> <p>13. Poluyanenko, N., Kuznetsov, A., Lisickiy, K., Datsenko, S., Nakisko, O., Rudenko, S., 2021. The Problem of Double Costs in Blockchain Systems, in: Hu, Z., Petoukhov, S., Dychka, I., He, M. (Eds.), Advances in Computer Science for Engineering and Education III, Advances in Intelligent Systems and Computing. Springer International Publishing, Cham, pp. 640–652. <a href="https://doi.org/10.1007/978-3-030-55506-1_57">https://doi.org/10.1007/978-3-030-55506-1_57</a></p> <p><b>П2 - Публ. аспіранта</b></p> <p>1. Кузнецов О.О., Тимченко В.А., Лисицький К.Є., Родінко М.Ю., Луценко М.С., Шеханін К.Ю., Колгатін А.О. Дослідження швидкодії та статистичної безпеки алгоритмів криптографічного гешування. Радіотехніка. 2019. Вип. 198. С. 75 — 95. DOI: 10.30837/rt.2019.3.198.06</p> <p>2. Kuznetsov A.A., Gorbenko Yu.I., Prokopovych-Tkachenko D.I., Lutsenko M.S., Pastukhov M.V. NIST PQC: Code-based Cryptosystems. Telecommunications and Radio Engineering. Begell House. 2019. С. 429 — 441. DOI: 10.1615/TelecomRadEng.v78.i5.50</p>
--	--	--	--

			<p>3. Lutsenko M.S. Code-based schemes presented at the 2nd round of the NIST PQC competition. IX Ukrainian Scientific Conference «Academic and scientific challenges of diverse fields of knowledge in the 21st century» (Kharkiv, February, 28, 2020).</p> <p>4. Луценко М.С. Пост квантовий алгоритм інкапсуляції ключів Classic McEliece. Радіотехніка. 2020. Вип. 203.</p>
6	Гармаш Дмитро Васильович, 2019, "Аналіз, обґрунтування, вибір та реалізація шифрів-кандидатів на роль основних криптографічних алгоритмів у квантовий період на основі мультіваріативних квадратичних перетворень"	Горбенко Іван Дмитрович	<p><b>ПІ - Публ. наукового керівника</b></p> <p>1. Gorbenko, I.D., Kachko, O.G., Yesina, M.V., 2018. Analysis of asymmetric NTRU Prime IT Ukraine encryption algorithm with regards to known attacks. Telecommunications and Radio Engineering, vol. 77. <a href="https://doi.org/10.1615/TelecomRadEng.v77.i9.50">https://doi.org/10.1615/TelecomRadEng.v77.i9.50</a></p> <p>2. Gorbenko, Y.I., Melnik, T.V., Gorbenko, I.D., 2018. Analysis of potential post-quantum schemes of hash-based digital signature. Telecommunications and Radio Engineering, vol. 77. <a href="https://doi.org/10.1615/TelecomRadEng.v77.i7.40">https://doi.org/10.1615/TelecomRadEng.v77.i7.40</a></p> <p>3. Gorbenko, I.D., Alekseychuk, A.N., Kachko, O.G., Yesina, M.V., Stelnik, I.V., Kandy, S.O., Bobukh, V.A., Ponomar, V.A., 2019a. Calculation of general parameters for NTRU Prime Ukraine of 6-7 levels of stability. Telecommunications and Radio Engineering, vol. 78. <a href="https://doi.org/10.1615/TelecomRadEng.v78.i4.40">https://doi.org/10.1615/TelecomRadEng.v78.i4.40</a></p> <p>4. Gorbenko, I.D., Kachko, O.G., Gorbenko, Y.I., Stelnik, I.V., Kandy, S.O., Yesina, M.V., 2019b. Methods of building general parameters and keys for NTRU Prime Ukraine of 5th – 7th levels of stability. Product form. Telecommunications and Radio Engineering, vol. 78. <a href="https://doi.org/10.1615/TelecomRadEng.v78.i7.30">https://doi.org/10.1615/TelecomRadEng.v78.i7.30</a></p> <p>5. Gorbenko, I., Kachko, O., Akolzina, O., 2018a. Research of post-quantum public key encryption algorithm, in: 2018 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo). Presented at the 2018 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo), pp. 1–4. <a href="https://doi.org/10.1109/UkrMiCo43733.2018.9047585">https://doi.org/10.1109/UkrMiCo43733.2018.9047585</a></p> <p>6. Gorbenko, I., Kachko, O., Yesina, M., Akolzina, O., 2018b. Post-quantum algorithm of asymmetric encryption and its basic properties,</p>

			<p>in: 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT). Presented at the 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), pp. 265–270. <a href="https://doi.org/10.1109/DESSERT.2018.8409142">https://doi.org/10.1109/DESSERT.2018.8409142</a></p> <p>7. Gorbenko, I., Kudryashov, I., Malieieva, H., 2018c. Comparative Analysis of Candidates for a Post-Quantum CPU Based on MQ Cryptographic Transformation, in: 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S T). Presented at the 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC ST), pp. 442–446. <a href="https://doi.org/10.1109/INFOCOMMST.2018.8632070">https://doi.org/10.1109/INFOCOMMST.2018.8632070</a></p> <p>8. Gorbenko I. Proposals of comparative analysis and decision making during the competition regarding the certain benefits of asymmetric post quantum cryptographic primitives / I. Gorbenko, Yu. Gorbenko, M. Yesina, V. Ponomar // COMPUTER SCIENCE AND CYBERSECURITY. – V. N. Karazin Kharkiv National University, 2017, Issue 1(5) – P. 53–70. Access mode: <a href="http://periodicals.karazin.ua/cscs/article/view/8307">http://periodicals.karazin.ua/cscs/article/view/8307</a>.</p> <p>9. Gorbenko I. Research of usage possibility and post-quantum algorithms advantages depend on application conditions / I. Gorbenko, Yu. Gorbenko, V. Ponomar, M. Yesina // COMPUTER SCIENCE AND CYBERSECURITY. – V. N. Karazin Kharkiv National University, 2017, Issue 3(7) – P. 45–66. Access mode: <a href="http://periodicals.karazin.ua/cscs/article/view/10005/9528">http://periodicals.karazin.ua/cscs/article/view/10005/9528</a>.</p> <p>11. Gorbenko I. D. NTRU Prime IIT Ukraine encryption algorithm with consideration known attacks analysis / I. D. Gorbenko, O.G. Kachko, M. V. Yesina // COMPUTER SCIENCE AND CYBERSECURITY. – V. N. Karazin Kharkiv National University, 2017, Issue 4(8) – P. 4–16. Access mode: <a href="https://periodicals.karazin.ua/cscs/article/view/10452/10192">https://periodicals.karazin.ua/cscs/article/view/10452/10192</a>.</p> <p>12. Gorbenko I. D. General statements and analysis of the end-to-end encryption algorithm NRTU Prime IIT Ukraine / I. D. Gorbenko, O. G.</p>
--	--	--	---



			<p>Kachko, M. V. Yesina // Radiotechnika. – Kh. : Kharkiv National University of Radio Electronics, 2018. – Issue 193 – P. 5–16.</p> <p>13. Gorbenko Ivan The problem of cryptographic transformations standardization and the state of its solution / Ivan Gorbenko, Olena Kachko, Oleksandr Kuznetsov, Yurii Gorbenko, Maryna Yesina // VII International Scientific and Technical Conference “Information protection and security of information systems”: Proceedings of the Scientific and Technical Conference, 30–31 May 2019. – L.: Lviv Polytechnic National University, 2019. – P. 84-85.</p> <p><b>П2 - Публ. аспіранта</b></p> <p>1. Доповідь на II науково-практичну конференцію “Проблеми кібербезпеки інформаційно-телекомунікаційних систем” на тему “Квантовий криптографічний алгоритм електронного підпису на основі мультіваріативних квадратичних перетворень”. Автори - Гармаш Д.В., Філатова Н.В., Горбенко І.Д., 23-24 березня, 2017.</p> <p>2. Стаття у журналі “Прикладна радіоелектроніка” на тему “Квантовий криптографічний алгоритм електронного підпису на основі мультіваріативних квадратичних перетворень”. Автори - Гармаш Д.В., Бакликов О.О., Філатова Н.В., Горбенко І.Д., 2016.</p> <p>3. Доповідь на науково-технічну міжнародну конференцію “Комп’ютерне моделювання у наукоємних технологіях (КМНТ-2021)” на тему “Генерація ключів і підпису за допомогою багатовимірного криптографічного алгоритму Rainbow”. Автори - Гармаш Д.В., Горбенко І.Д., 2021.</p> <p>4. Стаття у журналі “Прикладна радіоелектроніка” на тему “Проект стандарту електронного підпису Rainbow та його основні властивості і можливості щодо застосування”. Автори - Гармаш Д., Малєєва Г., Кандій С., 2021.</p> <p>5. Доповідь на конференцію «Технології захисту інформації та кіберзахисту» Військового інституту телекомунікацій та інформатизації імені Героїв Крут на тему “Криптографічні алгоритми на основі мультіваріативних квадратичних перетворень як кандидати на роль основних у пост-квантовий період”. Автори - Горбенко І.Д., Гармаш Д.В., 2020.</p>
--	--	--	---

			<p>6. Доповідь на конференцію “Безпека інформаційних систем і технологій (КМНТ-2018)” на тему “Пост-квантові алгоритми електронного підпису на основі мультіваріативних квадратичних перетворень. Схема підпису Rainbow”. Автори - Гармаш Д.В., Філатова Н.В., 2018.</p> <p>7. Стаття у журналі “Прикладна радіоелектроніка” на тему “Пост-квантові алгоритми електронного підпису та шифрування на основі мультіваріативних квадратичних перетворень”. Автори - Гармаш Д.В., Філатова Н.В., Горбенко І.Д., 2018.</p> <p>8. Доповідь на конференцію «Технології захисту інформації та кіберзахисту» Військового інституту телекомунікацій та інформатизації імені Героїв Крут на тему “Квантові криптографічні алгоритми електронного підпису на основі багатовимірних квадратичних перетворень”. Автори - Гармаш Д.В., Філатова Н.В., Горбенко І.Д., 2017.</p> <p>9. Доповідь на I міжнародну науково-практичну конференцію “Проблеми кібербезпеки інформаційно-телекомунікаційних систем (PCSITS)” на тему “Квантові криптографічні алгоритми шифрування та електронного підпису на основі мультіваріативних квадратичних перетворень”. Автори - Гармаш Д.В., Філатова Н.В., Горбенко І.Д., 2018</p> <p>10. Доповідь на III міжнародну науково-практичну конференцію “Проблеми кібербезпеки інформаційно-телекомунікаційних систем (PCSITS)” на тему “Оцінка стійкості та параметрів квантового алгоритму електронного підпису Rainbow”. Автори - Гармаш Д.В., Горбенко І.Д., 2020.</p>
7	Білозерцев Іван Микитович, 2019, "Моделі та методи криптографічного доведення з нульовим розголошенням із застосуванням алгебраїчних кодів"	Кузнецов Олександр Олександрович	<p><b>П1 - Публ. наукового керівника</b></p> <p>1. Gorbenko, I., Kuznetsov, A., Lutsenko, M., Ivanenko, D., 2017. The research of modern stream ciphers, in: 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S T). Presented at the 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S T), pp. 207–210. <a href="https://doi.org/10.1109/INFOCOMMST.2017.8246381">https://doi.org/10.1109/INFOCOMMST.2017.8246381</a></p>

			<p>2. Gorbenko, I., Kuznetsov, A., Tymchenko, V., Gorbenko, Y., Kachko, O., 2018a. Experimental Studies Of The Modern Symmetric Stream Ciphers, in: 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S T). Presented at the 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S T), pp. 125–128. <a href="https://doi.org/10.1109/INFOCOMMST.2018.8632058">https://doi.org/10.1109/INFOCOMMST.2018.8632058</a></p> <p>3. Gorbenko, I., Kuznetsov, A., Tymchenko, V., Gorbenko, Y., Kachko, O., 2018a. Experimental Studies Of The Modern Symmetric Stream Ciphers, in: 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S T). Presented at the 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S T), pp. 125–128. <a href="https://doi.org/10.1109/INFOCOMMST.2018.8632058">https://doi.org/10.1109/INFOCOMMST.2018.8632058</a></p> <p>4. Kuznetsov, A., Frolenko, V., Eremin, E., Zavgorodnia, O., 2018a. Research of cross-platform stream symmetric ciphers implementation, in: 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT). Presented at the 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), pp. 300–305. <a href="https://doi.org/10.1109/DESSERT.2018.8409148">https://doi.org/10.1109/DESSERT.2018.8409148</a></p> <p>5. Kuznetsov, A., Kiian, A., Gorbenko, Y., Smirnov, O., Cherep, O., Bexhter, L., 2019c. Code-based Pseudorandom Generator for the Post-Quantum Period, in: 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT). Presented at the 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT), pp. 204–209. <a href="https://doi.org/10.1109/ATIT49449.2019.9030493">https://doi.org/10.1109/ATIT49449.2019.9030493</a></p> <p>6. Kuznetsov, A., Lutsenko, M., Kuznetsova, K., Martyniuk, O., Babenko, V., Perevozova, I., 2019i. Statistical Testing of Blockchain Hash Algorithms, in: Fedushko, S., Gnatyuk, S., Peleshchyshyn, A., Hu, Z., Odarchenko, R., Korobiichuk, I. (Eds.), Proceedings of the International Workshop on Conflict Management in Global Information Networks (CMiGIN 2019) Co-Located with 1st International Conference on Cyber Hygiene and Conflict Management in Global</p>
--	--	--	---

			<p>Information Networks (CyberConf 2019), Lviv, Ukraine, November 29, 2019, CEUR Workshop Proceedings. CEUR-WS.org, pp. 67–79.</p> <p>7. Rassomakhin, S., Kuznetsov, A., Shlokin, V., Belozertsev, I., Serhiienko, R., 2018. Mathematical Model for the Probabilistic Minutia Distribution in Biometric Fingerprint Images, in: 2018 IEEE Second International Conference on Data Stream Mining Processing (DSMP). Presented at the 2018 IEEE Second International Conference on Data Stream Mining Processing (DSMP), pp. 514–518. <a href="https://doi.org/10.1109/DSMP.2018.8478496">https://doi.org/10.1109/DSMP.2018.8478496</a></p> <p>8. Shapoval, O., Kuznetsov, A., Poluyanenko, N., Yakovenko, V., Prokopovych-Tkachenko, D., Kavun, S., 2019. The Decentralized Voting Model Using the Hyperledger Platform Paper, in: 2019 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo). Presented at the 2019 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo), pp. 1–5. <a href="https://doi.org/10.1109/UkrMiCo47782.2019.9165368">https://doi.org/10.1109/UkrMiCo47782.2019.9165368</a></p> <p>9. Shekhanin, K., Kuznetsov, A., Krasnobayev, V., Smirnov, O., 2020. Detecting Hidden Information in FAT. IJCNIS 12, 33–43. <a href="https://doi.org/10.5815/ijcnis.2020.03.04">https://doi.org/10.5815/ijcnis.2020.03.04</a></p> <p>10. Shekhanin, K.Y., Kolhatin, A.O., Demenko, E.E., Kuznetsov, A.A., 2019. On Hiding Data Into The Structure Of The Fat Family File System. Tre 78. <a href="https://doi.org/10.1615/TelecomRadEng.v78.i11.50">https://doi.org/10.1615/TelecomRadEng.v78.i11.50</a></p> <p>11. Kuznetsov, O.O., Gorbenko, Y.I., Bilozertsev, I.M., Andrushkevych, A.V., Narizhnyi, O.P., 2018. ALGEBRAIC IMMUNITY OF NON-LINEAR BLOCKS OF SYMMETRIC CIPHERS. TRE 77. <a href="https://doi.org/10.1615/TelecomRadEng.v77.i4.30">https://doi.org/10.1615/TelecomRadEng.v77.i4.30</a></p> <p>12. Poluyanenko, N., Kuznetsov, A., Lazareva, E., Marakushyn, A., 2020. Extrapolation to calculate the probability of a double spending attack, in: Subbotin, S. (Ed.), Proceedings of The Third International Workshop on Computer Modeling and Intelligent Systems (CMIS-2020), Zaporizhzhia, Ukraine, April 27-May 1, 2020, CEUR Workshop Proceedings. CEUR-WS.org, pp. 610–620.</p> <p>13. Poluyanenko, N., Kuznetsov, A., Lisickiy, K., Datsenko, S., Nakisko, O., Rudenko, S., 2021. The Problem of Double Costs in</p>
--	--	--	---

Blockchain Systems, in: Hu, Z., Petoukhov, S., Dychka, I., He, M. (Eds.), *Advances in Computer Science for Engineering and Education III, Advances in Intelligent Systems and Computing*. Springer International Publishing, Cham, pp. 640–652. [https://doi.org/10.1007/978-3-030-55506-1\\_57](https://doi.org/10.1007/978-3-030-55506-1_57)

**П2 - Публ. аспіранта**

1. O.O. Kuznetsov, Yu.I. Gorbenko, I.M. Bilozertsev, A.V. Andrushkevych, O.P. Narizhnyi. "Algebraic Immunity of Non-linear Blocks of Symmetric Ciphers." *Telecommunications and Radio Engineering*, Volume 77, 2018, Issue 4, pp. 309-325.
2. Кузнецов А.А., Белозерцев И.Н., Андрушкевич А.В. Анализ и сравнительные исследования нелинейных узлов замены современных блочных симметричных шифров // *Прикладная радиоэлектроника*. – Харьков: ХНУРЭ. – 2015. – Том 14. №4. – С.343 – 350.
3. Кузнецов О.О., Горбенко Ю.И., Білозерцев І.М., Андрушкевич А.В., Наріжний О.П. Алгебраїчний імунітет нелінійних вузлів симетричних шифрів // *Радиотехника: Всеукр. межвед. науч.-техн. сб.* – Харьков: ХНУРЭ.–2017. – Вып. 189. – С. 47-58.
4. Kuznetsov, A. Kiian, I. Belozertsev, M. Pastukhov, D. Prokopovych-Tkachenko. Code-based schemes for digital signatures // *Computer science and cybersecurity*. – Kharkiv: V.N. Karazin Kharkiv National University. – Issue 2(10) 2018. – P. 23-31.
5. S. Rassomakhin, A. Kuznetsov, V. Shlokin, I. Belozertsev, R. Serhiienko. Probabilistic minutia distribution in biometric fingerprint images // *Computer science and cybersecurity*. – Kharkiv: V.N. Karazin Kharkiv National University. – Issue 2(10) 2018. – P. 32-39.
6. Kuznetsov, K. Shekhanin, A. Kolhatin, I. Mikheev and I. Belozertsev, "Hiding data in the structure of the FAT family file system," 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kyiv, Ukraine, 2018, pp. 337-342.
7. S. Rassomakhin, A. Kuznetsov, V. Shlokin, I. Belozertsev and R. Serhiienko, "Mathematical Model for the Probabilistic Minutia Distribution in Biometric Fingerprint Images," 2018 IEEE Second

			<p>International Conference on Data Stream Mining &amp; Processing (DSMP), Lviv, Ukraine, 2018, pp. 514-518.</p> <p>8. Кузнецов А.А., Белозерцев И.Н., Андрушкевич А.В. Нелинейные узлы замен блочных симметричных шифров // Моделирование-2016: сборник трудов конференции. – Киев, 2016. – С. 183-186.</p> <p>9. Кузнецов О.О., Иваненко Д.В., Белозерцев І.М., Андрушкевич А.В. Алгоритм потокового криптоперетворення «Струмок» // Труды научно-технической конференции с международным участием «Компьютерное моделирование в наукоемких технологиях», 26-31 мая 2016 г. – Х.: ХНУ имени В.Н. Каразина – 2016. – С. 187-190.</p> <p>10. Kuznetsov, I. Moskovchenko, I. Bilozertsev, S. Kavun, T. Kuznetsova. Heuristic Methods for the Design of Cryptographic Boolean Functions. In.: ISCI'2018: Information Security in Critical Infrastructures. Collective monograph. Edited by Ivan D. Gorbenko and Alexandr A. Kuznetsov, ASC Academic Publishing, USA, 2018, pp. 45-74. – ISBN: 978-0-9989826-5-6 (Paperback).</p> <p>11. Kuznetsov, A. Kiian, I. Bilozertsev, M. Pastukhov, D. Prokopovych-Tkachenko. Code-Based Schemes for Digital Signatures. In.: ISCI'2018: Information Security in Critical Infrastructures. Collective monograph. Edited by Ivan D. Gorbenko and Alexandr A. Kuznetsov, ASC Academic Publishing, USA, 2018, pp. 125-140. – ISBN: 978-0-9989826-5-6 (Paperback).</p> <p>12. I. Moskovchenko, A. Kuznetsov, S. Kavun, B. Akhmetov, I. Bilozertsev, S. Smirnov, HEURISTIC METHODS FOR THE DESIGN OF CRYPTOGRAPHIC BOOLEAN FUNCTIONS, International Journal of Computing. 18 (2019) 265–277</p>
8	Тимченко Владислав Анатолійович, 2018, "Моделі та методи потокового симетричного шифрування для захисту інформації в перехідний та постквантовий період"	Кузнецов Олександр Олександрович	<p><b>П1 - Публ. наукового керівника</b></p> <p>1 Кузнецов О.О. Дослідження кросплатформних реалізацій потокових симетричних шифрів / Кузнецов О.О., Фроленко В.О., Єрьомін Є.С., Иваненко Д.В. // Радиотехника: Всеукр. міжвед. науч.-техн. сб. – 2018. – №193. – С. 94–106.</p>

			<p>2 Kuznetsov A. Output Feedback Encryption Mode: Periodic Features of Output Blocks Sequence / A. Kuznetsov, Y. Gorbenko, I. Kolovanova, S. Smirnov, I. Perevozova, T. Kuznetsova // Lecture Notes on Data Engineering and Communications Technologies, 2021, 48, pp. 621–648.</p> <p>3 Кузнецов О.О. Дослідження поточкових алгоритмів шифрування – переможців міжнародного проекту eStream / Кузнецов О.О., Іваненко Д.В., Мордвінов // Прикладная радиоэлектроника, 2015, Том 14, № 4. – С. 321 – 334.</p> <p>4 Горбенко І.Д. Статистичні властивості блокових симетричних шифрів з міжнародного стандарту ISO/IEC 29192-2 / Горбенко І.Д., Кузнецов О.О., Самойлова А.В. // Радиотехника. 2014. Вып. 176. – С. 40 – 44.</p> <p>5 Кузнецов О.О. Порівняльні дослідження алгоритмів поточкового криптографічного перетворення / Кузнецов О.О., Іваненко Д.В., Луценко М.С., Тимченко В.А., Мелкозерова О.М., Осадчук М.О., Остряньська Є.В. // Радиотехника. 2017. Вып. 191. – С. 52 – 75.</p> <p><b>П2 - Публ. аспіранта</b></p> <p>1. Кузнецов О.О. Математична структура поточкового шифру Струмок / Кузнецов О.О., Горбенко І.Д., Горбенко Ю.І., Олексійчук А.М., Тимченко В.А. // Радиотехніка: Всеукр. міжвід. наук.-техн. зб. 2018. Вип. 193. С. 17 – 27.</p> <p>2. Кузнецов О.О. Експериментальні дослідження сучасних поточкових симетричних шифрів / Кузнецов О.О., Тимченко В.А., Фроленко В.О., Єрьомін Є.С. // Міжнародна науково-практична конференція 14-15 березня 2018 року, м. Харків. С. 94 – 96.</p> <p>3. Gorbenko I. Testing the speed of modern stream ciphers / I. Gorbenko, Y. Gorbenko, V. Tymchenko, O. Kachko // Computer Science And Cybersecurity, ISSUE 3(11) 2018, pp. 48 – 55. ISSN 2519-2310 (Online).</p> <p>4. Gorbenko I. Experimental Studies of the Modern Symmetric Stream Ciphers / I. Gorbenko, A. Kuznetsov, V. Tymchenko, Y. Gorbenko, O. Kachko // 2018 International Scientific-Practical Conference on</p>
--	--	--	---

			<p>Problems of Infocommunications Science and Technology, PIC S and T 2018 - Proceedings, 2019, pp. 125–128.</p> <p>5. Gorbenko I. Strumok keystream generator / I. Gorbenko, O. Kuznetsov, Y. Gorbenko, A. Alekseychuk, V. Tymchenko // Proceedings of 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies, DESSERT 2018, 2018, pp. 294–299.</p> <p>6. Gorbenko I. "Strumok" Stream Cipher. Testing the Speed and Statistical Properties / I. Gorbenko, A. Kuznetsov, Y. Gorbenko, A. Alekseychuk, V. Tymchenko // In.: ISCI'2018: Information Security in Critical Infrastructures. Collective monograph. Edited by Ivan D. Gorbenko and Alexandr A. Kuznetsov, ASC Academic Publishing, USA, 2018, pp. 14-44. – ISBN: 978-0-9989826-5-6 (Paperback).</p> <p>7. Gorbenko I. Studies on statistical analysis and performance evaluation for some stream ciphers / I. Gorbenko, A. Kuznetsov, Y. Gorbenko, S. Vdovenko, V. Tymchenko, M. Lutsenko // International Journal of Computing, 2019, 18(1), pp. 82–88.</p> <p>8. Gorbenko I. Testing the Speed of Modern Stream Ciphers / I. Gorbenko, A. Kuznetsov, Y. Gorbenko, V. Tymchenko // ISCI 2019: Information Security In Critical Infrastructures. Collective monograph. Edited by Ivan D. Gorbenko and Alexandr A. Kuznetsov, ASC Academic Publishing, USA, 2019, pp. 39 – 47. – ISBN: 978-0-9989826-8-7 (Hardback).</p> <p>9. Горбенко І.Д. Спосіб потокового симетричного шифрування / Горбенко І.Д., Кузнецов О.О., Горбенко Ю.І., Олексійчук А.М., Тимченко В.А. // Патент на винахід № 120472. Зареєстровано в Державному реєстрі патентів України на винаходи 10.12.2019.</p> <p>10. Кузнецов О.О. Дослідження швидкодії та статистичної безпеки алгоритмів криптографічного гешування / Кузнецов О.О., Тимченко В.А., Лисицький К.Є., Родінко М.Ю., Луценко М.С., Шеханін К.Ю., Колгатін А.О. // Радіотехніка: Всеукр. міжвід. наук.-техн. зб. 2019. Вип. 198. С. 75 – 95.</p> <p>11. Kuznetsov A. Performance of Hash Algorithms Suitable for Use in Blockchain / A. Kuznetsov, V. Tymchenko, K. Lisitskiy, M. Rodinko // ISCI 2019: Information Security In Critical Infrastructures. Collective</p>
--	--	--	--



			monograph. Edited by Ivan D. Gorbenko and Alexandr A. Kuznetsov, ASC Academic Publishing, USA, 2019, pp. 199 – 210. – ISBN: 978-0-9989826-8-7 (Hardback).
9	Вілігура Владислав Вікторович, 2018, "Моделі та методи забезпечення безпеки баз даних з універсальним базисом відношень"	1-2 курс – Єсін Віталій Іванович 3-4 курс – Рассомахін Сергій Геннадійович	<p><b>П1 - Публ. наукового керівника</b></p> <ol style="list-style-type: none"> <li>1. Есин В. И. Кибернетический подход к решению задачи реинжиниринга баз данных / В. И. Есин // Радиотехника: Всеукр. межвед. науч.-техн. сб. – 2017. Вып. 189. – С. 15-22.</li> <li>2. Есин В. И. Выразительные средства модели данных «объект-событие» В. И. Есин // Радиотехника: Всеукр. межвед. науч.-техн. сб. – 2017. Вып. 191. – С. 99-112.</li> <li>3. Есин В. И. Модель данных «объект-событие»: требования и синтез модели // Computer science and cyber security – International electronic scientific journal. – 2017. – Issue. 3 (7). – P. 33-44, <a href="http://periodicals.karazin.ua/cscs/article/view/">http://periodicals.karazin.ua/cscs/article/view/</a></li> <li>4. Security and noise immunity of telecommunication systems: new solutions to the codes and signals design problem. Collective monograph. Edited by Sergey G. Rassomakhin and A.A. Kuznetsov – Minden, Nevada, USA : ASC Academic Publishing. – 2017. – 198 p. (Chapter 8, Yesin V. I., Yesina M. V.).</li> <li>5. Есин В. И. Инвариантная к предметным областям схема базы данных и ее отличительные особенности / В. И. Есин // Радиотехника: науч.-техн. журнал. – 2018, Вып. 193. – С. 133-142.</li> <li>6. Yesin V. I. A cybernetic approach to solving the problem of database reengineering // Telecommunications and Radio Engineering. – 2018. Volume 77, Issue 5. – P. 399-409. doi: 10.1615/TelecomRadEng.v77.i5.40. (Scopus)</li> <li>7. Yesin V.I., Yesina M.V., Rassomakhin S.G., Karpinski M. (2018) Ensuring Database Security with the Universal Basis of Relations. In: Saeed K., Homenda W. (eds) Computer Information Systems and Industrial Management. CISIM 2018. Lecture Notes in Computer Science, vol. 11127. Springer, Cham, Chapter 42, P. 510-522. DOI 10.1007/978-3-319-99954-8_42. (Scopus, Web of Science)</li> </ol>

			<p>8. Есин В. И. Метод разработки баз данных, легко адаптируемых к изменениям в предметной области / В. И. Есин, В. В. Вилигура // Радиотехника: науч.-техн. журнал. – 2018, Вып. 195. – С. 184-192.</p> <p>9. Есин В. И. Метод преобразования унаследованных баз данных в базу данных с универсальным базисом отношений / В. И. Есин, В. В. Вилигура // Прикладная радиоэлектроника. – 2018. – Т. 17, № 3, 4. С. 176-181.</p> <p>10. Yesin V. I., Vilihura V. V. Method for development of databases easily adaptable to variations in the subject domain // Telecommunications and Radio Engineering. – 2019. Volume 78, Issue 7. – P. 595-605. DOI: 10.1615/TelecomRadEng.v78.i7.40. (Scopus)</p> <p>11. Стислий словник основних термінів з безпеки інформаційних систем, технологій, кібербезпеки / уклад. В. І. Єсін, С. Г. Рассомахін. – Харків : ХНУ імені В. Н. Каразіна, 2018. – 64 с.</p> <p>12. Yesin V. I. Some approach to data masking as means to counter the inference threat / V. I. Yesin, V. V. Vilihura // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2019. – № 198. – P. 113-130.</p> <p>13. Yesin V. I. Formalized representation for the data model with the universal basis of relations / V. I. Yesin, M. Karpinski, M. V. Yesina, V. V. Vilihura // International Journal of Computing, 2019. – № 18(4). – P. 453-460. (Scopus)</p> <p>14. Есин В. И. Обратимое маскирование больших двоичных объектов, хранящихся в базе данных / В. И. Есин, В. В. Вилигура // Прикладна радіоелектроніка: наук.–техн. журнал. – 2019. – Т. 18, № 3, 4. С. 154-164.</p> <p>15. V.I. Yesin, M.V. Yesina, V.V. Vilihura Monitoring the integrity and authenticity of stored database objects // Telecommunications and Radio Engineering. – 2020. Volume 79, Issue 12. – P. 1029-1054. DOI: 10.1615/TelecomRadEng.v79.i12.20 (Scopus)</p> <p>16. Vitalii Yesin, Mikolaj Karpinski, Maryna Yesina, Vladyslav Vilihura and Kornel Warwas Hiding the Source Code of Stored Database Programs // Information. 2020. Volume 11, Issue 12, 576. DOI: 10.3390/info11120576. (Scopus)</p> <p>17. Technology for Developing Databases of Information Systems / [V. M. Grachev, V. I. Esin, N. G. Polukhina, S. G. Rassomahin] // Bulletin</p>
--	--	--	---

			<p>of the Lebedev Physics Institute. – New York, USA : Allerton Press, Inc. (Distributed worldwide by Springer) – 2014. – Vol. 41. – № 5. – P. 119-122. (Scopus, Web of Science)</p> <p>18. Data Security Mechanisms Implemented in the Database with Universal Model / [V. M. Grachev, V. I. Esin, N. G. Polukhina, and S. G. Rassomakhin] // Bulletin of the Lebedev Physics Institute. – New York, USA : Allerton Press, Inc. (Distributed worldwide by Springer) – 2014. – Vol. 41. – № 5. – P. 123-126. (Scopus, Web of Science)</p> <p>19. Рассомахин С. Г. Выбор технологии организации хранения и использования данных в информационных системах определенного класса / С. Г. Рассомахин, В. И. Есин, М. В. Есина // Параллельная компьютерная алгебра и её приложения в новых инфокоммуникационных системах: I-я Международная конференция, сборник научных трудов, 20-24 октября 2014 г., г. Ставрополь, Россия, Северо-Кавказский федеральный университет. – Ставрополь : Издательско-информационный центр «Фабула», 2014. – С. 156-160.</p> <p>20. Есин В. И. Разработка механизмов, обеспечивающих защиту информации в базах данных / В. И. Есин, В. В. Вилигура // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління. Матеріали восьмої міжнародної науково-технічної конференції, 26-27 квітня 2018 г. – Полтава, Баку, Харків, Жиліна, 2018. – С. 58.</p> <p>21. Есин В. И. Анализ устойчивости к взлому системы парольной защиты СУБД Oracle / В. И. Есин, Д. О. Ганжа // Перспективні напрямки сучасної електроніки, інформаційних і комп'ютерних систем (MEICS-2018). Тези доповідей на III Всеукраїнській науково-практичній конференції: 21-23 листопада 2018 р. – Дніпро, Дніпровський національний університет імені Олеся Гончара, Кременчук: ПП Щербатих О. В., 2018. – С. 74-75.</p> <p>22. Vitalii I. Yesin, Mikolaj Karpinski, Maryna V. Yesina, Vladyslav V. Vilihura, Olga Veselska, Lukasz Wieclaw Approach to Managing Data From Diverse Sources // Proceedings of the 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), 18-21</p>
--	--	--	--

September, 2019, Metz, France, Volume 1, P. 1-6. (Scopus, Web of Science)

**П2 - Публ. аспіранта**

1. Есин В. И., Вилигура В. В. Метод разработки баз данных, легко адаптируемых к изменениям в предметной области // Радіотехніка: наук.-техн. журнал. – 2018, Вип. 195. – С. 184-192.
2. Есин В. И., Вилигура В. В. Метод преобразования унаследованных баз данных в базу данных с универсальным базисом отношений // Прикладна радіоелектроніка. – 2018. – Т. 17, № 3, 4. С. 176-181.
3. Yesin V. I., Vilihura V. V. Method for development of databases easily adaptable to variations in the subject domain // Telecommunications and Radio Engineering. – 2019. Volume 78, Issue 7. – P. 595-605. DOI: 10.1615/TelecomRadEng.v78.i7.40. (входит до бази Scopus).
4. V. V. Vilihura Some approach to data masking as means to counter the inference threat / V. I. Yesin, V. V. Vilihura // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2019. – № 198. – P. 113-130.
5. V. V. Vilihura Formalized representation for the data model with the universal basis of relations / V. I. Yesin, M. Karpinski, M. V. Yesina, V. V. Vilihura // International Journal of Computing, 2019. – № 18(4). – P. 453-460 (входит до бази Scopus).
6. В. В. Вилигура Обратимое маскирование больших двоичных объектов, хранящихся в базе данных / В. И. Есин, В. В. Вилигура // Прикладна радіоелектроніка: наук.-техн. журнал. – 2019. – Т. 18, № 3, 4. С. 154-164.
7. V.I. Yesin, M.V. Yesina, V.V. Vilihura Monitoring the integrity and authenticity of stored database objects // Telecommunications and Radio Engineering. – 2020. Volume 79, Issue 12. – P. 1029-1054. DOI: 10.1615/TelecomRadEng.v79.i12.20 (входит до бази Scopus)
8. Vitalii Yesin, Mikolaj Karpinski, Maryna Yesina, Vladyslav Vilihura and Kornel Warwas Hiding the Source Code of Stored Database Programs // Information. 2020. Volume 11, Issue 12, 576. DOI: 10.3390/info11120576. (входит до бази Scopus)

			<p>9. Вилигура В. В., Есин В. И., Рассомахин С. Г. Анализ формальных моделей управления доступом и особенности их применимости для баз данных // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021.</p> <p>10. Вилигура В. В., Есин В. И., Рассомахин С. Г. Анализ формальных моделей обеспечения целостности данных и их применимость для баз данных // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021.</p> <p>11. Есин В. И. Разработка пакета подпрограмм для проведения исследований блочных симметричных шифров в СУБД Oracle / В. И. Есин, В. В. Вилигура // Теоретичні та прикладні аспекти побудови програмних систем : матеріали міжнародної наукової конференції, м. Київ, 23-26 листопада 2015 р. – Кіровоград : ПП «Центр оперативної поліграфії «Авангард»», 2015. – С. 58-64.</p> <p>12. Вілігура В. В. Використання національного криптоалгоритму для захисту персональних даних в СУБД Oracle / В. В. Вілігура, В. І. Єсін // Компьютерное моделирование в наукоемких технологиях (КМНТ-2016) : Труды научно-технической международной конференции, 26-31 мая 2016 г. – Х. : Харьковский национальный университет имени В. Н. Каразина, 2016. – С. 77–80.</p> <p>13. Есин В. И. Разработка механизмов, обеспечивающих защиту информации в базах данных / В. И. Есин, В. В. Вилигура // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління. Матеріали восьмої міжнародної науково-технічної конференції, 26-27 квітня 2018 г. – Полтава, Баку, Харків, Жиліна, 2018. – С. 58.</p> <p>14. Vitalii I. Yesin, Mikolaj Karpinski, Maryna V. Yesina, Vladyslav V. Vilihura, Olga Veselska, Lukasz Wieclaw Approach to Managing Data from Diverse Sources // 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Metz, France, September 18-21, 2019 (входить до бази Scopus, Web of Science)</p> <p>15. Єсіна М. В. Аналіз та можливості застосування технології блокчейн / М. В. Єсіна, В. А. Бобух, В. В. Вілігура // Проблеми кібербезпеки інформаційно-телекомунікаційних систем (PCSITS):</p>
--	--	--	--

			<p>Праці III Міжнародної науково-практичної конференції, 12 червня 2020 р. – К. : Київський національний університет імені Тараса Шевченка, 2020. – С. 237-241.</p> <p>16. В. В. Вілігура, Ю. І. Горбенко, В. І. Єсін, С. Г. Рассомахін Використання формальних моделей безпеки в захищених базах даних / Міжнародна наукова конференція «Питання оптимізації обчислень (ПОО-XLVII)», 21–24 вересня 2021 року (на базі Національного університету «Львівська політехніка»).</p> <p>17. В. В. Вілігура Систематизація загроз і вразливостей інформаційної безпеки актуальних для баз даних і СУБД / Науково-технічна міжнародна конференція «Комп'ютерне моделювання у наукоємних технологіях (КМНТ-2021)», 21-23 квітня 2021 року (на базі Харківського національного університету імені В.Н. Каразіна).</p> <p>Звіти про НДР:</p> <p>18. «Механізми, методи, протоколи та засоби криптографічного захисту інформації у пост квантовий період» (Шифр «Квант-2019»). Огляд та аналіз усіх основних перспективних методів та стандартів симетричного шифрування, в тому числі для постквантового періоду. Новий підхід до маскуванню даних, що зберігаються в базах і сховищах даних (проміжний).</p> <p>19. «Механізми, методи, протоколи та засоби криптографічного захисту інформації у пост квантовий період» (Шифр «Квант-2019», Том 5). Огляд та аналіз усіх основних перспективних методів та стандартів симетричного шифрування, в тому числі для постквантового періоду. Підхід до забезпечення конфіденційності і цілісності даних об'єктів певного класу, що зберігаються в базах і сховищах даних (заклучний).</p> <p>20. «Механізми та засоби електронного підпису у пост квантовий період» (Шифр «Квант-2020», Том 5). Удосконалений метод забезпечення конфіденційності і цілісності даних об'єктів певного класу, що зберігаються в базах і сховищах даних. Розробка механізмів контролю цілісності та автентичності збережених в БД об'єктів, що ґрунтуються на можливостях технології блокчейн (проміжний).</p>
--	--	--	---

			21. «Механізми та засоби електронного підпису у пост квантовий період» (Шифр «Квант-2020», Том 4). Програмні моделі, базового та оптимізованого програмного забезпечення (бібліотек) перспективних криптопримітивів ЕП для постквантового періоду. Формальні моделі безпеки і їх застосовність для БД (заключний).
10	Колгатін Андрій Олександрович, 2018, "Програмно-апаратні засоби захисту цифрового контенту що базуються на кластерних файлових системах"	Кузнецов Олександр Олександрович	<p><b>П1 - Публ. наукового керівника</b></p> <ol style="list-style-type: none"> <li>1. Kuznetsov, A., Shekhanin, K., Smirnov, O., &amp; Chepurko, I. (2019). Detecting Hidden Information in FAT. ISCI'2019: Information Security In Critical Infrastructures, 412.</li> <li>2. Shekhanin, K., Kuznetsov, A., Krasnobayev, V., &amp; Smirnov, O. (2020). Detecting Hidden Information in FAT. International Journal of Computer Network &amp; Information Security, 12(3).</li> <li>3. Kuznetsov, A., Smirnov, O., Onikiychuk, A., Makushenko, T., Anisimova, O., &amp; Arischenko, A. (2020, May). Adaptive Pseudo-Random Sequence Generation for Spread Spectrum Image Steganography. In 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT) (pp. 161-165). IEEE.</li> <li>4. Kuznetsov, A., Shekhanin, K., Kolhatin, A., Mikheev, I., &amp; Belozertsev, I. (2018, May). Hiding data in the structure of the FAT family file system. In 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT) (pp. 337-342). IEEE.</li> <li>5. Kuznetsov, A., Shekhanin, K., Kolhatin, A., Kovalchuk, D., Babenko, V., &amp; Perevozova, I. (2019, December). Performance of hash algorithms on gpus for use in blockchain. In 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT) (pp. 166-170). IEEE.</li> <li>6. Кузнецов, О. О., Тимченко, В. А., Лисицький, К. Є., Родінко, М. Ю., Луценко, М. С., Шеханін, К. Ю., &amp; Колгатін, А. О. (2019). Дослідження швидкодії та статистичної безпеки алгоритмів криптографічного гешування. Радіотехніка, 3(198), 75-95.</li> <li>7. Kuznetsov, A., Shekhanin, K., Kolgatin, A., Kuznetsova, K., &amp; Demenko, Y. (2018). Hiding data in the file structure. Комп'ютерні науки та кібербезпека, (1), 43-52.</li> </ol>

			<p>8. Shekhanin, K. Y., Kolhatin, A. O., Demenko, E. E., &amp; Kuznetsov, A. A. (2019). On Hiding Data Into the Structure of the FAT Family File System. <i>Telecommunications and Radio Engineering</i>, 78(11).</p> <p>9. Kuznetsov, A. A., Stefanovych, O. O., Prokopovych-Tkachenko, D. I., &amp; Kuznetsova, K. O. (2019). 3D steganography information hiding. <i>Telecommunications and Radio Engineering</i>, 78(12).</p> <p>10. Кузнецов, О. О., Горбенко, Ю. І., Онопрієнко, В. В., Стельник, І. В., &amp; М'ялковський, Д. В. (2019). Дослідження алгоритмів криптографічного гешування, які застосовуються в сучасних блокчейн-системах. <i>Радіотехніка</i>, 3(198), 54-74.</p> <p>11. Смірнов, О., Арищенко, А., Деменко, Є., Онікійчук, О., &amp; Кузнецов, О. (2019). Псевдовипадкові дискретні послідовності для стеганосистем з використанням технології прямого розширення спектра. <i>Комп'ютерні науки та кібербезпека</i>, (4), 4-10.</p> <p><b>П2 - Публ. аспіранта</b></p> <p>1. Shekhanin, K., Kolhatin, A., Kuznetsova, K., &amp; Kavun, S. (2018, September). Steganographic hiding information in a file system structure. In <i>2018 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo)</i> (pp. 1-6). IEEE.</p> <p>2. Kuznetsov, A., Shekhanin, K., Kolhatin, A., Mikheev, I., &amp; Belozertsev, I. (2018, May). Hiding data in the structure of the FAT family file system. In <i>2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)</i> (pp. 337-342). IEEE.</p> <p>3. Kuznetsov, A., Shekhanin, K., Kolhatin, A., Kovalchuk, D., Babenko, V., &amp; Perevozova, I. (2019, December). Performance of hash algorithms on gpus for use in blockchain. In <i>2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT)</i> (pp. 166-170). IEEE.</p> <p>4. Шеханин, К. Ю., Колгатин, А. А., &amp; Деменко, Е. Е. Стеганографический Метод Проверки Подлинности Аппаратных Средств Хранения Данных. Матеріали ІХ-ої Міжнародної науково-практичної конференції «Free and Open Source Software», Харків,</p>
--	--	--	---



			<p>21-23 листопада 2017 р.–Харків: Харківський національний університет будівництва та архітектури, 2017.–112 с., 97.</p> <p>5. Кузнецов, О. О., Тимченко, В. А., Лисицький, К. Є., Родінко, М. Ю., Луценко, М. С., Шеханін, К. Ю., &amp; Колгатін, А. О. (2019). Дослідження швидкодії та статистичної безпеки алгоритмів криптографічного гешування. Радіотехніка, 3(198), 75-95.</p> <p>6. Шеханін, К. Ю., Колгатін, А. О., Деменко, Є. Є., &amp; Кузнецов, О. О. (2018). Приховування даних у структуру файлової системи сімейства FAT. Радіотехніка, 2(193), 169-178.</p> <p>7. Kuznetsov, A., Shekhanin, K., Kolgatin, A., Kuznetsova, K., &amp; Demenko, Y. (2018). Hiding data in the file structure. Комп'ютерні науки та кібербезпека, (1), 43-52.</p> <p>8. Shekhanin, K. Y., Kolhatin, A. O., Demenko, E. E., &amp; Kuznetsov, A. A. (2019). On Hiding Data Into the Structure of the FAT Family File System. Telecommunications and Radio Engineering, 78(11).</p>
11	Кулібаба Владислав Андрійович, 2018, "Методи, моделі та засоби побудування постквантових криптографічних протоколів інкапсуляції ключів по критеріям-безпеки- складність"	Горбенко Іван Дмитрович	<p><b>ПІ - Публ. наукового керівника</b></p> <p>1. Comparative Analysis of Candidates for a Post-Quantum CPU Based on MQ Cryptographic Transformation Gorbenko, I., Kudryashov, I., Malieieva, H. 2018 International Scientific-Practical Conference on Problems of Infocommunications Science and Technology, PIC S and T 2018 - Proceedings, 2019, стр. 442–446, 8632070</p> <p>2. Methods of building general parameters and keys for NTRU Prime Ukraine of 5th – 7th levels of stability. Gorbenko, I.D., Kachko, O.G., Gorbenko, Yu.I., ...Kandy, S.O., Yesina, M.V. Telecommunications and Radio Engineering (English translation of Elektrosvyaz and Radiotekhnika), 2019, 78(7), стр. 579–594</p> <p>3. Calculation of general parameters for NTRU Prime Ukraine of 6-7 levels of stability. Gorbenko, I.D., Alekseychuk, A.N., Kachko, O.G., ...Bobukh, V.A., Ponomar, V.A. Telecommunications and Radio Engineering (English translation of Elektrosvyaz and Radiotekhnika), 2019, 78(4), стр. 327–340</p> <p>4. Research of post-quantum public key encryption algorithm Gorbenko, I., Kachko, O., Akolzina, O. 2018 International Conference</p>

			<p>on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo 2018 - Proceeding, 2018, 9047585</p> <p>5. Post-quantum algorithm of asymmetric encryption and its basic properties Gorbenko, I., Kachko, O., Yesina, M., Akolzina, O. Proceedings of 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies, DESSERT 2018, 2018, стр. 265–270</p> <p>6. Gorbenko I.D., Kachko O.G, Alekseychuk A.N., Kuznetsov O.O., Gorbenko Yu.I., Onoprienko V.V., Yesina M.V., Candiy S.O. Algorithms of asymmetric encryption and encapsulation of keys of post-quantum period of 5 -7 levels of stability and their applications // Radiotekhnika. Kharkov : KNURE, 2019. Is. 198. P. 5-18. DOI:10.30837/rt.2019.3.198.01.</p> <p><b>П2 - Публ. аспіранта</b></p> <p>1. Сутність та умови здійснення атаки на зв'язаних ключах відносно електронних підписів IBS-1 та IBS-2 ДСТУ ISO/IEC 14888-3 - Сутність та умови здійснення атаки на зв'язаних ключах відносно електронних підписів IBS-1 та IBS-2 ДСТУ ISO/IEC 14888-3 / Ю. І. Горбенко, М. В. Єсіна, В. А. Кулібаба // Системи обробки інформації. — 2016. — № 7. — С. 113-118. (<a href="http://www.hups.mil.gov.ua/periodic-app/article/16934">http://www.hups.mil.gov.ua/periodic-app/article/16934</a>)</p> <p>2. Аналіз механізмів підпису на основі геш-функцій. – Матеріали VI Міжнародної НТК «Захист інформації безпека інформаційних систем» 2017р.</p> <p>3. Огляд та аналіз основних пост квантових механізмів підпису на основі геш-функцій – Матеріали XIX Міжнародної НТК «Безпека інформації у інформаційно-телекомунікаційних системах» 2017р.</p> <p>4. Стійкість алгоритмів електронного підпису стандарту ISO 14888:2014 проти атак на зв'язаних ключах – Матеріали міжнародної НТК «Комп'ютерное моделирование в наукоемких технологиях» 2017р.</p> <p>5. Аналіз стійкості електронних підписів IBS-1 та IBS-2 ДСТУ ISO/IEC 14888-3 проти атаки на зв'язаних ключах / Горбенко І.Д., Кулібаба В.А. // матеріали XI НАУКОВО-ПРАКТИЧНОЇ</p>
--	--	--	--

			<p>КОНФЕРЕНЦІЇ „Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення. Застосування підрозділів, комплексів, засобів зв'язку та автоматизації в операції Об'єднаних сил” 8 – 9 листопада 2018 року</p> <p>6. Аналіз сутності та моделі протоколу інкапсуляції ключів у кільці поліномів над скінченим полем / Горбенко І. Д., Качко О. Г., Пономар В. А., М. В., Акользіна О. С., Кулібаба В. А. // Прикладна радіоелектроніка: Науково-технічний журнал, 2018, Том 17, № 3, 4</p> <p>7. Порівняльний аналіз криптоперетворень на еліптичних кривих та кривих Едвардса / В.А. Кулібаба, // Радіотехніка: Всеукр. міжвід. наук.-техн. зб. 2019. Вип. 198. С. 203—208.</p> <p>8. Ivan Gorbenko, Vladyslav Kulibaba, Mariia Dron. The essence of the method and properties of asymmetric encryption and key encapsulation algorithms in a polynomials ring over a finite field in new project of DSTU standard. // MATERIALS of VIIth International Scientific and Technical Conference “Information Protection And Information Systems Security” 2019</p> <p>9. Процеси та методи вибору загальносистемних параметрів перспективного алгоритму електронного підпису на основі алгебраїчних решіток. / Кулібаба, В. А. // Радіотехніка, Вип. 202, 64–71. 2020. <a href="https://doi.org/10.30837/rt.2020.3.202.06">https://doi.org/10.30837/rt.2020.3.202.06</a></p> <p>10. Перспективні методи та системи криптографічного захисту інформації / О.М. Олексійчук, В.А. Кулібаба, М.В. Єсіна, С. О. Кандій, Є.В. Остряньська, І.Д. Горбенко // Радіотехніка. – 2020. – Вип. 200. – С. 5-13.</p>
12	Шеханін Кирило Юрійович, 2017, "Розробка та аналіз стеганографічних методів приховування даних в структуру файлових систем"	Кузнецов Олександр Олександрович	<p><b>П1 - Публ. наукового керівника</b></p> <p>1. Gorbenko, I., Kuznetsov, A., Lutsenko, M., Ivanenko, D., 2017. The research of modern stream ciphers, in: 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S T). Presented at the 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S T), pp. 207–210. <a href="https://doi.org/10.1109/INFOCOMMST.2017.8246381">https://doi.org/10.1109/INFOCOMMST.2017.8246381</a></p>

			<p>2. Gorbenko, I., Kuznetsov, A., Tymchenko, V., Gorbenko, Y., Kachko, O., 2018a. Experimental Studies Of The Modern Symmetric Stream Ciphers, in: 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S T). Presented at the 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S T), pp. 125–128. <a href="https://doi.org/10.1109/INFOCOMMST.2018.8632058">https://doi.org/10.1109/INFOCOMMST.2018.8632058</a></p> <p>3. Gorbenko, I., Kuznetsov, A., Tymchenko, V., Gorbenko, Y., Kachko, O., 2018a. Experimental Studies Of The Modern Symmetric Stream Ciphers, in: 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S T). Presented at the 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S T), pp. 125–128. <a href="https://doi.org/10.1109/INFOCOMMST.2018.8632058">https://doi.org/10.1109/INFOCOMMST.2018.8632058</a></p> <p>4. Kuznetsov, A., Frolenko, V., Eremin, E., Zavgorodnia, O., 2018a. Research of cross-platform stream symmetric ciphers implementation, in: 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT). Presented at the 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), pp. 300–305. <a href="https://doi.org/10.1109/DESSERT.2018.8409148">https://doi.org/10.1109/DESSERT.2018.8409148</a></p> <p>5. Kuznetsov, A., Kiian, A., Gorbenko, Y., Smirnov, O., Cherep, O., Bexhter, L., 2019c. Code-based Pseudorandom Generator for the Post-Quantum Period, in: 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT). Presented at the 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT), pp. 204–209. <a href="https://doi.org/10.1109/ATIT49449.2019.9030493">https://doi.org/10.1109/ATIT49449.2019.9030493</a></p> <p>6. Kuznetsov, A., Lutsenko, M., Kuznetsova, K., Martyniuk, O., Babenko, V., Perevozova, I., 2019i. Statistical Testing of Blockchain Hash Algorithms, in: Fedushko, S., Gnatyuk, S., Peleshchyshyn, A., Hu, Z., Odarchenko, R., Korobiichuk, I. (Eds.), Proceedings of the International Workshop on Conflict Management in Global Information Networks (CMiGIN 2019) Co-Located with 1st International Conference on Cyber Hygiene and Conflict Management in Global</p>
--	--	--	---

			<p>Information Networks (CyberConf 2019), Lviv, Ukraine, November 29, 2019, CEUR Workshop Proceedings. CEUR-WS.org, pp. 67–79.</p> <p>7. Rassomakhin, S., Kuznetsov, A., Shlokin, V., Belozertsev, I., Serhiienko, R., 2018. Mathematical Model for the Probabilistic Minutia Distribution in Biometric Fingerprint Images, in: 2018 IEEE Second International Conference on Data Stream Mining Processing (DSMP). Presented at the 2018 IEEE Second International Conference on Data Stream Mining Processing (DSMP), pp. 514–518. <a href="https://doi.org/10.1109/DSMP.2018.8478496">https://doi.org/10.1109/DSMP.2018.8478496</a></p> <p>8. Shapoval, O., Kuznetsov, A., Poluyanenko, N., Yakovenko, V., Prokopovych-Tkachenko, D., Kavun, S., 2019. The Decentralized Voting Model Using the Hyperledger Platform Paper, in: 2019 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo). Presented at the 2019 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo), pp. 1–5. <a href="https://doi.org/10.1109/UkrMiCo47782.2019.9165368">https://doi.org/10.1109/UkrMiCo47782.2019.9165368</a></p> <p>9. Shekhanin, K., Kuznetsov, A., Krasnobayev, V., Smirnov, O., 2020. Detecting Hidden Information in FAT. IJCNIS 12, 33–43. <a href="https://doi.org/10.5815/ijcnis.2020.03.04">https://doi.org/10.5815/ijcnis.2020.03.04</a></p> <p>10. Shekhanin, K.Y., Kolhatin, A.O., Demenko, E.E., Kuznetsov, A.A., 2019. On Hiding Data Into The Structure Of The Fat Family File System. Tre 78. <a href="https://doi.org/10.1615/TelecomRadEng.v78.i11.50">https://doi.org/10.1615/TelecomRadEng.v78.i11.50</a></p> <p>11. Kuznetsov, O.O., Gorbenko, Y.I., Bilozertsev, I.M., Andrushkevych, A.V., Narizhnyi, O.P., 2018. Algebraic immunity of non-linear blocks of symmetric ciphers. TRE 77. <a href="https://doi.org/10.1615/TelecomRadEng.v77.i4.30">https://doi.org/10.1615/TelecomRadEng.v77.i4.30</a></p> <p>12. Poluyanenko, N., Kuznetsov, A., Lazareva, E., Marakushyn, A., 2020. Extrapolation to calculate the probability of a double spending attack, in: Subbotin, S. (Ed.), Proceedings of The Third International Workshop on Computer Modeling and Intelligent Systems (CMIS-2020), Zaporizhzhia, Ukraine, April 27-May 1, 2020, CEUR Workshop Proceedings. CEUR-WS.org, pp. 610–620.</p> <p>13. Poluyanenko, N., Kuznetsov, A., Lisickiy, K., Datsenko, S., Nakisko, O., Rudenko, S., 2021. The Problem of Double Costs in</p>
--	--	--	---

Blockchain Systems, in: Hu, Z., Petoukhov, S., Dychka, I., He, M. (Eds.), Advances in Computer Science for Engineering and Education III, Advances in Intelligent Systems and Computing. Springer International Publishing, Cham, pp. 640–652. [https://doi.org/10.1007/978-3-030-55506-1\\_57](https://doi.org/10.1007/978-3-030-55506-1_57)

**П2 - Публ. аспіранта**

1. Hiding data in the structure of the FAT family file system  
Published in: 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT) Date of Conference: 24-27 May 2018. SCOPUS  
<https://ieeexplore.ieee.org/abstract/document/8409155>
2. On hiding data into the structure of the fat family file system  
Begellhouse DOI: 10.1615/TelecomRadEng.v78.i11.50 pages 973-985 <http://www.dl.begellhouse.com/journals/0632a9d54950b268,3b40033676b88971,345b224a73de0f10.html>
3. Performance of Hash Algorithms on GPUs for Use in Blockchain  
Published in: 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT) Date of Conference: 18-20 Dec. 2019 SCOPUS <https://ieeexplore.ieee.org/abstract/document/9030442>
4. Detecting Hidden Information in FAT I. J. Computer Network and Information Security, 2020, 3, 33-43 Published Online June 2020 in MECS (<http://www.mecs-press.org/>) Published By: MECS Press IJCNIS Vol.12, No.3, Jun. 2020 DOI: 10.5815/ijcnis.2020.03.04 <http://j.mecs-press.net/ijcnis/ijcnis-v12-n3/IJCNIS-V12-N3-4.pdf>
5. Steganographic hiding information in a file system structure  
Published in: 2018 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo) SCOPUS  
<https://ieeexplore.ieee.org/abstract/document/9047551>

			<p>6. Hiding Data In The File Structure. ISSN 2519-2310XXX-XXXXCS&amp;CS, Issue 1(9) 2018. <a href="https://periodicals.karazin.ua/cscs/article/view/12013">https://periodicals.karazin.ua/cscs/article/view/12013</a></p> <p>7. ISCI'2019: Information Security In Critical Infrastructures. Collective monograph Chapter 27 Detecting Hidden Information in FAT <a href="https://osf.io/u3bt4/download#page=413">https://osf.io/u3bt4/download#page=413</a></p> <p>8. Приховування даних у структуру файлової системи сімейства FAT Радіотехніка #193 (2018) <a href="http://rt.nure.ua/article/view/175804">http://rt.nure.ua/article/view/175804</a></p> <p>9. Дослідження швидкодії та статистичної безпеки алгоритмів криптографічного гешування Радіотехніка #198 (2019) <a href="http://rt.nure.ua/article/view/184661">http://rt.nure.ua/article/view/184661</a></p> <p>10. Приховування інформації шляхом перемішування кластерів у файловій системі FAT32 Міністерство освіти і науки України Одеська національна академія зв'язку ім. О.С. Попова 71-ша науково-технічна конференція професорсько-викладацького складу, науковців, аспірантів та студентів <a href="https://biblio.onat.edu.ua/bitstream/handle/123456789/1781/2016%20%D0%BA%D0%BE%D0%BD%D1%84.%D0%A71.PDF?sequence=1&amp;isAllowed=y#page=112">https://biblio.onat.edu.ua/bitstream/handle/123456789/1781/2016%20%D0%BA%D0%BE%D0%BD%D1%84.%D0%A71.PDF?sequence=1&amp;isAllowed=y#page=112</a></p> <p>11. Kirill Shekhanin, Lyudmila Gorbachova, Alexander Kuznetsov Comparative Analysis and Study of Storage Devices Properties for Steganographic Data Hiding in Cluster File Systems Ministry Of Education And Science Of Ukraine Lviv Polytechnic National University National Aviation University 2nd International Conference on Cyber Hygiene &amp; Conflict Management in Global Information Networks November 30, 2020.</p>
--	--	--	---