



«CHALLENGES AND THREATS TO CRITICAL INFRASTRUCTURE»



Detroit (Michigan, USA) - 2023

Challenges and threats to critical infrastructure. Collective monograph - [NGO Institute for Cyberspace Research](#) (Detroit, Michigan, USA), 2023. - 325 p.

The collective monograph was prepared by ukrainian scholars within the framework of studies of a wide range of security issues. The authors of the monograph look at the problems of security of the state`s security in a rich manner behind such basic warehouses as military security, information security, military-technical security, environmental and technogenic security

Reviewers:

Ponomarev S.P. - Doctor of Jurisprudence, head of the Department of Administration of the State Service of Special Communications and Information Protection of Ukraine

Hnatyuk S.O. - Ph.D. Chief Researcher of the State Scientific and Research Institute of Cybersecurity Technologies and Information Protection

Silvestrov A.M. - Ph.D. Prof. National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”

© Collective of Authors, 2023
© NGO Institute for Cyberspace Research, 2023
ISBN-10/979-8-218-22315-1

Authors

Chapter 1. Avramenko O.V., Polishchuk V.V., Sarapin Yu.O., Voinov I.A. 1, V.A. Malik, N.V. Zhenyuk, N.I. Voropai, O.G. Korol, A.Yu. Strelnikova, Yu.V. Kostenko, O.V. Peredrii, V.V. Gordiychuk, Grinenko O.I., Hrytsyuk V.V., Zubkov V.P., Ptashkin R.L., Palagin V.V., Savostyanenko M.V., Klymenko K.V., Klymenko K.V., Tyutyunyk V. ., Kapelushna T.V.

Chapter 2. Azarenko O., Honcharenko Yu., Divizinyuk M., Shevchenko R., Shevchenko O., V.M. Vashchenko, V.I. Skalozubov, I.B. Korduba, Shcherbak O., Khmyrova A., Khrystych V., Zhuk V. M., Pohosyan G. A., Yevlanov M. V., Cherepnyov I. A., Chumachenko S. M., Kolomiets D. P., Matsko P. I., Kaplia I. O., Romanyuk V. P., Medvedev M. G., Mulyava O. M., Peredrii O. V., Komisarov M. V., Proshchyn I. V., Sydorenko V .L., Eremenko S.A., Tyshchenko V.O., Vlasenko E.A., Pruskyi A.V., Demkiv A.M., Yudina D.O.

Chapter 3. V. N. Yelisieiev, E. V. Bykova, V. S. Tyshchenko, N. V. Zaika, V. A. Popel, S. S. Chumachenko, O. V. Ivchenko, V. V. Palagin, R. Kyrychok. V., Laptev O.A., Laptev S.O., Sobchuk A.V., Ponomarenko V.V., Barabash A.O., Murasov R.K., Chumachenko S.M., Sirik A.O. , Yevtushenko O.V., Sobchuk V.V., Pichkur V.V., Lapteva T.O., Kopytko S.B.

Chapter 4. Goncharenko I.O., Kuchma T.L., Prodanyuk D.M., Zaretskyi I.S., Karpenko M.I., Moshenskyi A.O., Derman V.A., Khoperskyi S. V., Chumachenko S.M., Ponomarenko S.O., Popel V.A, Maslennikova T.A.

Chapter 5. Vovchuk T., Shevchenko R., Shevchenko O., Guida O.G., Kiselyov V.B., Ometsynska N.V., Trysnyuk T.V., Konetska O.O., Nagornyi E. I., Marushchak V.M., Volynets T.V., Prystupa V.V., Trofimchuk O.M., Trysnyuk V.M., Shumeiko V.O., Chumachenko S.M., Lysenko O.I. , O. M. Tachynina, O. V. Furtat, S. O. Furtat, I. O. Sushin.

Chapter 6. Viola Vambol, Alina Kowalczyk-Juško, Sergij Vambol, Nadeem Ahmad Khan, Aaron Dumont, Zaporozhchenko M.M., Legominova S.V., Muzhanova T.M., Ometsynska N.V., Kiselyov V. B., Huida O. G., Shchavinskyi Y.V., Palchynska V.B.

Chapter 7. Altaf Hussain Lahori, Barbara Savytska, Parisa Ziarati, Barbara Krokhmal-Marchak, Niloofar Mozaffari, Nastaran Mozaffari, Miasoyedova A., Divizinyuk M., Shevchenko R., Myroshnychenko A., Aldoshin O.O., Kalinovskyy A.Ya., Vykhatin M.V., Havrys A.P., R.S. Yakovchuk, O.O. Pekarska, M.V. Yevlanov, R.V. Antoshchenkov, I.A. Cherepnyov, I.I. Kravchenko, V. Loik. B., Synelnikov O.D., Goncharenko M.O., Nazarenko S.Yu., Mandrychenko D.S., Shapovalov M.M., Pichugin M.A., Vynogradov S.A., Samchenko T.V. , Nuyanzin O.V., Sverchkov O.V., Faure E.V., Skutskyi A.B., Lavdanskyi A.O., Grechanyk O.S., Shakhov S.M., Zinchenko O.O., Yatsenko V.O., Vambol S.O.

Chapter 8. Adamova G.V., Anila Kausar, Ambreen Afza, Altaf Hussain Lahori, Bobkov Y.V., Shevchuk A.A., Stamati V.G., Vynogradov S.A., Chumachenko S.M., Lysenko O.I., Novikov V.I., Furtat O.V., Furtat S.O., Sushin I.O., Pisnya L.A., Mishchenko I.V., Vambol S.O., Vambol Viola

Chapter 9. Yakovliev Ye.O., Rudko G.I., Yermakov V.M., Chumachenko S.M., Kodryk A.I., Dyatel O.O., Lubenska N.O.

CONTENT

CHAPTER 1 SYSTEMATIC APPROACH TO THE PROTECTION OF CRITICAL INFRASTRUCTURE FACILITIES	9
1. Avramenko O.V., Polishchuk V.V., Sarapin Yu.O. Increasing the efficiency of protection of ammunition storage facilities against emergency situations by implementing justified periodic maintenance of fire protection systems.....	10
2. Voinov I.A. 1, Malik V.A. A systematic approach to the protection of critical infrastructure objects	13
3. Zhenyuk N.V., Voropai N.I., Korol O.G., Strelnikova A.Yu. Security model of sociocyberphysical system	16
4. Yu. V. Kostenko Green tariff as a tool for improving the security of critical infrastructure facilities	18
5. Peredrii O.V., Gordiychuk V.V., Grinenko O.I., Hrytsyuk V.V., Zubkov V.P. Integration of foreign and domestic mechanisms for ensuring cyber security of critical infrastructure objects	21
6. Ptashkin R.L., Palagin V.V. Cross-layer web application security concept.....	25
7. Savostyanenko M.V., Klymenko K.V. Regulatory aspects of the identification and categorization of critical infrastructure facilities	27
8. Tarnavskiy A.B. Emergency situations of tpp turbogenerators and their prevention ways	31
9. Tyutyunyk V.V., Yashchenko O.A., Tyutyunyk O.O. Development of the support system for anti-crisis decisions under the conditions of the implementation of the legal regime of martial or state of emergency	35
10. Faure E.V., Makhynko M.V. Approaches to construct error-correcting permutation code for non-separable factorial data coding.....	40
11. Khokhlacheva Yu.E., Gavrilova A.A. Analysis of information security threats in modern information and communication systems and networks	42
12. Yakymenko Yu.M., Rabchun D.I., Kapelyushna T.V. Use of methodological approaches of system analysis to ensure information security of critical infrastructure objects	46
CHAPTER 2 THEORETICAL AND METHODOLOGICAL BASIS OF ASSESSMENT OF CYBER THREATS, TECHNOLOGICAL AND ENVIRONMENTAL THREATS AND RISKS FOR CRITICAL INFRASTRUCTURE	52
13. Azarenko O., Honcharenko Yu., Divizinyuk M., Shevchenko R., Shevchenko O. Generalization of the characteristics of critical state infrastructure objects	53
14. V.M. Vashchenko, V.I. Skalozubov, I.B. Korduba Nuclear and ecological danger of the Zaporizhzhya NPP in the extreme conditions of the war in Ukraine	54
15. Shcherbak O., Khmyrova A., Khrystych V., Shevchenko R. Methods of identifying the main signs of an extraordinary situation at critical infrastructure facilities	59
16. Zhuk V. M., Pohosyan G. A. Some issues of flooding risk management	60
17. Yevlanov M.V., Cherepnyov I.A., Chumachenko S.M., Kolomiets D.P. Some aspects of increasing the shelf life and efficiency of using food concentrates in extreme conditions.....	63

18. Matsko P. I., Kaplya I. O., Romanyuk V. P. Theoretical and methodological basis for assessing man-made threats and risks to the critical infrastructure of Ukraine under the conditions of a full-scale invasion of the Russian Federation.....	68
19. Medvedev M.G., Mulyava O.M. Investigation of geometric properties of differential equations with complex coefficients.....	71
20. Peredrii O.V., Komisarov M.V. Procedure for assessing the efficiency of measures for cleaning critical infrastructure objects from explosive objects during war.....	75
21. Proshchyn I.V. Analysis of factors which are involved in the causes of accidents at hydrotechnical sports.....	80
22. Sydorenko V.L., Yeremenko S.A., Tyshchenko V.O., Vlasenko E.A. Methodological bases of risk assessment of emergency situations at potentially dangerous facilities of critical infrastructure.....	84
23. Sydorenko V.L., Pruskyi A.V., Demkiv A.M. Development of the risk of hazards at industrial facilities of critical infrastructure.....	87
24. Yudina D.O. Cybersecurity measures for critical information infrastructure facilities against cyber threats and cyber attacks.....	89
CHAPTER 3 METHODS AND TOOLS FOR ASSESSMENT OF CYBER THREATS, TECHNOLOGICAL AND ENVIRONMENTAL THREATS AND RISKS FOR CRITICAL INFRASTRUCTURE.....	94
25. Yelisieev V.N., Bykova E.V. Issues of assessment of man-made or environmental risks for critical infrastructure objects.....	95
26. Tyshchenko V.S. Methodology of using neural networks for analyzing cyber security threats and critical infrastructure operations.....	99
27. Zaika N.V., Popel V.A., Chumachenko S.S. Assessment of the security level of critical infrastructure based on the complex of tools to protect its objects against UAV.....	101
28. Ivchenko O.V., Palagin V.V. Network security threats at data link level.....	105
29. Kyrychok R.V., Laptev O.A. Methodology for confirming the feasibility of exploiting detected vulnerabilities in a corporate network using polynomial transformations of Bernstein.....	107
30. Laptev S.O., Sobchuk A.V., Ponomarenko V.V., Barabash A.O. Parametric method of spectral analysis of signals of critical infrastructure objects.....	111
31. Murasov R.K., Chumachenko S.M. Risk assessment of critical infrastructure facilities, taking into account the potentials of losses from the destructive influence of the enemy.....	114
32. Sirik A.O., Yevtushenko O.V. Safety requirements and technological threats for food industry enterprises as critical infrastructure facilities.....	122
33. Sobchuk V.V., Pichkur V.V., Lapteva T.O., Kopytko S.B. Method of increasing the immunity of the system of detection and recognition of radio signals for objects of critical infrastructure.....	127
CHAPTER 4 SOFTWARE TOOLS FOR ANALYTICS, CYBER THREATS MODELING SYSTEMS, TECHNOLOGICAL AND ENVIRONMENTAL PROCESSES AND ACTIVITIES OF CRITICAL INFRASTRUCTURE FACILITIES.....	131

34. Honcharenko I.O., Kuchma T.L., Prodanyuk D.M. Knowledge, attitudes, and practices assessment of public bomb shelter use in Kyivska Oblast	132
35. Zaretsky I.S. Modeling indicators of investment systems	146
36. Karpenko M.I., Chumachenko S.M., Moshenskyi A.O. Substantiating of the components for creating a software and hardware complex for detection of radiation and chemical warfare agents	152
37. Khoperskyi S.V., Chumachenko S.M., Ponomarenko S.O., Popel V.A., Maslennikova T.A. A model for the restoration of territories with critical infrastructure damaged by military actions	156
CHAPTER 5 INFORMATION SYSTEMS FOR ASSESSMENT OF CYBER THREATS, TECHNOLOGICAL AND ENVIRONMENTAL THREATS AND RISKS FOR CRITICAL INFRASTRUCTURE	159
38. Vovchuk T., Shevchenko R., Shevchenko O. Information technologies for the prevention of emergency situations at chemical industry facilities	160
39. Huida O.G., Kiselyov V.B., Ometsynska N.V. Information systems for evaluating cybersecurity threats	161
40. Trysnyuk T.V., Konetska O.O., Nagorny E.I., Marushchak V.M., Volynets T.V., Prystupa V.V. Assessment of the radiation risk of contamination of the area for the population as a result of military operations	163
41. Trofymchuk O.M., Trysnyuk V.M., Shumeiko V.O. Surface water bodies of Ukraine as part of critical infrastructure facilities under the conditions of Russian aggression	167
42. Chumachenko S.M., Lysenko O.I., Tachynina O.M., Furtat O.V., Furtat S.O., Sushin I.O. Method of collecting information on the condition of critical infrastructure objects from wireless sensor network nodes	171
CHAPTER 6 INTERNATIONAL STANDARDS IN THE FIELD OF INFORMATION AND TELECOMMUNICATION TECHNOLOGIES AND CYBER PROTECTION OF CRITICAL INFRASTRUCTURE FACILITIES	179
43. Viola Vambol, Alina Kowalczyk-Juško, Sergij Vambol, Nadeem Ahmad Khan Current state of the potential for waste to energy conversion: overview of the situation in Poland	180
44. Aaron Dumont Environmental protection through international criminal law ...	184
45. Zaporozhchenko M.M. Legislation in the field of cyber protection of critical infrastructure facilities	188
46. Legominova S.V., Muzhanova T.M. Secure handling protected critical infrastructure information: the US experience	191
47. Ometsynska N.V., Kiselyov V.B., Huida O.G. Features of the dynamic spectrum expansion of the optical transmitter	195
48. Shchavinskyi Y.V., Palchynska V.B. Legal mechanisms for ensuring cyber protection of objects of critical information infrastructure of Ukraine in conditions of hybrid war	198
CHAPTER 7 MODELING AND SIMULATION OF NATURAL DISASTERS, EMERGENCIES AND THEIR RESPONSE	203

49. Miasoyedova A., Divizinyuk M., Shevchenko R. Mathematical models for detecting the danger of critical infrastructure objects by unmanned aerial vehicles.....	204
50. Myroshnychenko A., Shevchenko R. Informational methods of emergency prevention due to explosion in tunnels.....	205
51. Aldoshin O.O., Kalinovskiy A.Ya. Problems of managing the creation and purchase of fire-fighting equipment.....	206
52. Vykhvatin M.V. Simulation of restoration systems of safe life activities in conditions of disaster risk.....	209
53. Havrys A.P., Yakovchuk R.S., Pekarska O.O. Visualization of Fire in Space and Time on the Basis of the Method of Spatial Location of Fire-Dangerous Areas.....	215
54. Evlanov M.V., Antoschenkov R.V., Cherepnyov I.A. On the need to create a register of mathematical models of the human body to improve the effectiveness of diagnostics in the field of disaster medicine.....	219
55. Kalinovskiy A.Ya., Kravchenko I.I. Fundamentals of using fire trucks.....	223
56. Loik V.B., Synelnikov O.D., Honcharenko M.O. Measures for the protection of the population and organization of the response during the liquidation of the consequences of the use of tactical nuclear weapons.....	226
57. Nazarenko S.Yu., Mandrychenko D.S. Concerning the use and design of a gear pump for fire extinguishing.....	230
58. Nazarenko S.Yu., Shapovalov M.M. Measuring complex for determining the hydraulic resistance of pressure fire hoses.....	232
59. Pichugin M.A., Vinogradov S.A. Use of transparent partitions for fire spread limitations in shopping and entertainment centers.....	234
60. Samchenko T.V., Nuyanzin O.V. Analysis of applied cfd and fem programs with their characteristics for cable tunnels.....	236
61. Kalinovskiy A.Ya., Sverchkov O.V. A systematic approach to assessing the level of readiness of units of the operational rescue service of civil protection.....	241
62. Faure E. V., Skutskiy A. B., Lavdanskyy A. O. Simulation model for text and audio messages transmission in the Simulink environment using non-separable factorial coding.....	244
63. Cherepnev I.A., Barbara Savytska, Parisa Ziarati, Barbara Krokhmal-Marchak, Vambol S.O. Technical measures to reduce grain losses at the storage stage from biotic factors.....	247
64. Cherepnev I.A., Vambol S.O., Niloofar Mozaffari, Nastaran Mozaffari The results of experimental studies of the effectiveness of remote radiothermometry in the field of medicine of emergency situations.....	251
65. Shakhov S.M., Grechanyk O.S. Development of an autonomous compressed air foam system.....	254
66. Shakhov S.M., Zinchenko O.O. Study of the efficiency of compressed air foam generation with domestic foam formers.....	258
67. Yatsenko V.O., Vinogradov S.A. On the issue of protection of personnel in the cab of a fire rescue vehicle from dangerous factors of fire.....	261

CHAPTER 8 EXPERIENCE IN USING INFORMATION TECHNOLOGIES, UAVs AND ROBOTS FOR ENVIRONMENTAL MONITORING, PREVENTION

AND ELIMINATION OF NATURAL AND MAN-MADE THREATS FOR CRITICAL INFRASTRUCTURE OBJECTS 263

68. Bobkov Yu.V., Shevchuk A.A. Use of UAVs and Modern Information Technologies to Monitor Fields in Precision Agriculture 264

69. Stamati V.G., Vinogradov S.A. Problems of fire extinguishing at energy facilities and ways to solve them 269

70. Tyutyunyk V.V., Tyutyunyk O.O., Usachov D.V. Geoinformation system for acoustic monitoring of different sources of threats for objects of critical infrastructure of the city 271

71. Chumachenko S.M., Lysenko O.I., Novikov V.I., Furtat O.V., Furtat S.O., Sushin I.O. Development of the method of support and increase of connectivity wireless networks using UAVs 277

72. Adamova G.V., Pisnya L.A. Environmental safety of operation of motor roads of ukraine. Assessment methods and tools and cyber security 284

73. Mishchenko I.V., Vambol S.O., Vambol V.V. Construction waste management during the territories reconstruction in order to environment protection 302

74. Anila Kausar, Ambreen Afza, Altaf Hussain Lahori, Viola Vambol Application of object based technique for assessment of urban land-use/land cover and air quality 306

CHAPTER 9 CHALLENGES AND THREATS TO CRITICAL INFRASTRUCTURE DURING OPERATION AND CLOSURE OF COAL MINES 311

75. Yakovliev Ye.O., Rudko G.I. Threats of a state of ecological chaos for critical infrastructure facilities in Donbass and Kryvbass under conditions of Russian aggression 312

76. Yermakov V.M., Chumachenko S.M., Kodryk A.I., Yakovlev E.O. Environmental and geological factors of the vulnerability of critical infrastructure objects under the conditions of Russian aggression 317

77. Dyatel O.O., Lubenska N.O., Ermakov V.M. Restructuring of mines of donbas in the conditions of military actions 321

10. ПІДХОДИ ДО ПОБУДОВИ ЗАВАДОСТІЙКОГО ПЕРЕСТАНОВОЧНОГО КОДУ ДЛЯ НЕРОЗДІЛЬНОГО ФАКТОРІАЛЬНОГО КОДУВАННЯ ДАНИХ

Фауре Е.В.¹, Махинько М.В.²

1 Черкаський державний технологічний університет, Черкаси, Україна
ГО «Інститут дослідження кіберпростору»

2 GoodLabs Studio Inc., Toronto, ON M5H 3E5, Canada

E-mail: e.faure@chdtu.edu.ua

Approaches to construct error-correcting permutation code for non-separable factorial data coding

The report highlights approaches to construct error-correcting permutation code in the context of its use in integrated data protection systems against channel errors and unauthorized access based on non-separable factorial coding. The use of affine and projective general linear groups to form an ensemble of permutations, in addition to providing a given code distance for permutation dictionaries (arrays), allows generating network and session keys during secure data exchange. The statistical approach to construct permutation code is based on enumerating permutations and selecting those permutations, which distance does not exceed a given value to all previously selected codewords.

Передавання коротких пакетів є ключовою особливістю сучасних бездротових систем, наднадійних і сенсорних мереж, масових комунікацій машинного типу (МТС), IoT застосувань. Поширеність таких систем і мереж у сучасному світі вимагає створення нових і адаптацію існуючих підходів до забезпечення цілісності та конфіденційності переданої інформації. Зокрема, потужність необхідних ресурсів для каналного кодування та криптографічного захисту, а також їх швидкодія відіграють подекуди визначальну роль.

Ця робота розглядає підходи до побудови завадостійких перестановочних кодів [1, 2] у контексті використання їх у системах інтегрованого захисту інформації від помилок каналу зв'язку та несанкціонованого доступу на основі нероздільного факторіального кодування даних [3, 4]. Такі перестановочні коди можуть бути використані, зокрема, з метою формування ансамблю кодових символів факторіального коду для інформаційної взаємодії об'єктів МТС з динамічно змінюваною структурою, а також забезпечення надійного передавання перестановок у складних заводових умовах, утому числі, для трьохетапного криптографічного протоколу на основі перестановок [5].

Множину перестановок на Z_M будемо називати масивом перестановок [6] і позначати через S_M . Відстань між перестановками $\pi_i, \pi_j \in S_M$ будемо позначати

через D_{ij} . Тоді завадостійким перестановочним кодом (M, D_{min}) є код, утворений підмножиною перестановок масиву S_M , де попарна відстань між перестановками π_i, π_j цієї підмножини задовольняє нерівності $D_{ij} \geq D_{min}$. Потужність коду (M, D_{min}) позначимо через $N(M, D_{min})$.

Спершу розглянемо алгоритми формування кодів $(M, M-1)$ і $(M+1, M-1)$ з простим M для досягнення $N(M, M-1) = M(M-1)$ і $N(M+1, M-1) = (M+1)M(M-1)$.

Код $(M, M-1)$ утворюється афінною загальною лінійною групою $AGL(1, M) = \{ax + b \mid a, b, x \in GF(M), a \neq 0\}$ [6] і з простим M породжується будь-яким елементом (перестановкою) цього коду, тобто якщо $S_M = \{ax + b, a, b \in Z_M, a \neq 0\}$ і $\sigma \in S_M$, то $\{a\sigma_x + b, a, b \in Z_M, a \neq 0\} = S_M$.

Код $(M+1, M-1)$ утворюється проєктивною загальною лінійною групою $PGL(2, M) = \left\{ f(x) = \frac{ax+b}{cx+d} \mid a, b, c, d \in GF(M), x \in GF(M) \cup \infty, ad \neq bc \right\}$ [6] і з простим M породжується будь-яким елементом (перестановкою) цього коду,

тобто якщо $S_{M+1} = \left\{ f(x) = \frac{ax+b}{cx+d} \mid a, b, c, d \in Z_M, x \in Z_M \cup \infty, ad \neq bc \right\}$ і $\sigma \in S_{M+1}$, то $\left\{ f(x) = \frac{a\sigma_x + b}{c\sigma_x + d} \mid a, b, c, d \in Z_M, ad \neq bc \right\} = S_{M+1}$.

Застосування афінної та проєктивної загальної лінійної груп для формування алфавіту повідомлень (перестановок), окрім забезпечення кодової відстані $M-1$ для словників (масивів) перестановок S_M і S_{M+1} , дозволяє формувати мережні та сеансові ключі під час захищеного обміну даними.

Статистичний підхід [7] до формування (M, D_{min}) -коду та оцінювання його потужності $N(M, D_{min})$ базується на переборі множини перестановок $\{\pi\}$ довжини M і відборі тих перестановок, відстань від яких не перевищує значення D_{min} до всіх відібраних до цього кодових слів.

Для забезпечення можливості побудови коду (M, D_{min}) за значень M , для яких реалізувати практично формування $M!$ перестановок неможливо, початкова множина перестановок представляє собою деяку власну підмножину потужності N_{lim} повної множини з $M!$ перестановок.

Експериментально визначені залежності середнього та максимального значень потужності $N(M, D_{min}, N_{lim})$ коду (M, D_{min}) , утвореного за підмножиною

з N_{lim} перестановок, від значення N_{lim} , а також методика побудови апроксимаційних квадратичних поліномів для визначених залежностей можуть бути використані для екстраполяції цих залежностей і прогнозування їх поведінки.

Література

1. Blake I. Permutation codes for discrete channels / I. Blake // IEEE Trans. Inf. Theory. – 1974. – Issue 20, No. 1. – P. 138–140.
2. Smith D. H. A new table of permutation codes / D. H. Smith, R. Montemanni // Des. Codes Cryptogr. – 2012. – Issue 63, No 2. – P. 241–253.
3. Faure E. V. Factorial coding with data recovery / E. V. Faure // Visnyk Cherkaskogo Derzhavnogo Tehnol. Univ. – 2016. – No. 2. – P. 33–39.
4. Faure E. V. Factorial coding with error correction / E. V. Faure // Radio Electron. Comput. Sci. Control. – 2017. – Issue 3. – P. 130–138.
5. Shcherba A. Three-Pass Cryptographic Protocol Based on Permutations / A. Shcherba, E. Faure, O. Lavdanska // 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (ATIT). – Kyiv, Ukraine : IEEE, 2020.
6. Mojica de la Vega L. G. Permutation Arrays with Large Hamming Distance / L. G. Mojica de la Vega. – The University of Texas at Dallas, 2017. – 106 p.
7. Faure E. Permutation-Based Block Code for Short Packet Communication Systems / E. Faure, A. Shcherba, M. Makhynko, B. Stupka, J. Nikodem, R. Shevchuk // Sensors. – 2022. – Issue. 22, No. 14, 5391.

УДК 336.74

11. АНАЛІЗ ЗАГРОЗ БЕЗПЕКИ ІНФОРМАЦІЇ В СУЧАСНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ І МЕРЕЖАХ

Хохлачова Ю. Є.¹, Гаврилова А. А.²

1 Національний авіаційний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна

2 Національний технічний університет «Харківський політехнічний інститут», Харків, Україна

E-mail: yuliiahohlachova@gmail.com, sharaya1972@gmail.com

Analysis of information security threats in modern information and communication systems and networks

Threats to information security and the consequences of their implementation in the form of cyberattacks were analyzed, and attractive directions for cybercriminals by sphere of activity were clarified. The dynamics of changes in the activity of cybercriminals are considered. As a result, it