

ЗМІСТ

<i>Бушков В.Г.</i> Моделювання стійкості електронних комунікацій до гібридних кібератак: підходи та сценарний аналіз витривалості інфраструктури.....	8
<i>Гайдур Г.І., Гамза Д.Є.</i> Гібридний метод виявлення шкідливої активності на основі стекінг-ансамблю класифікаторів.....	20
<i>Гапон А. О.</i> Експериментальне дослідження, програмна реалізація та оцінка ефективності застосування методу захисту програмного забезпечення на основі гібридного аналізу.....	27
<i>Гончаров М.О., Нарєжний О.П., Малахов С.В.</i> Аналіз передумов для забезпечення консенсусу ресурсів при виконанні процедур вставлення стеганографічних даних.....	37
<i>Дейнека О. Р., Гарасимчук О. І.</i> Agile підхід до впровадження методології збору, обробки, зберігання та класифікації даних у відповідності до вимог SOC2 Type2.....	48
<i>Домарєв В.В., Прокопович-Ткаченко Д.І, Зверев В.П., Бушков В.Г, Козаченко І.М.</i> Ситуаційно-орієнтовані системи управління безпекою на основі уніфікованої матричної моделі: логіко-лінгвістичний та міжгалузовий підхід.....	56
<i>Журавель Ю.І., Онишко В.Р.</i> Підвищення ефективності стеганографічної системи через застосування методів обробки зображень.....	68
<i>Іваночко Т. А., Семенюк С. А.</i> Управління ризиками кібербезпеки з використанням NIST CSF 2.0.....	75
<i>Лантєв О.А., Стеценко В. О.</i> Метод побудови криптосистеми нідеррайтера на основі М-кодів.....	83
<i>Легомінова С.В., Капелюшина Т.В., Щавінський Ю.В., Мужанова Т.М.</i> Концептуальні підходи інтеграції етичних норм у політику інформаційної безпеки.....	90
<i>Лозова І.Л., Різак М.В., Хохлачова Ю.Є., Котик О.В.</i> Аналіз моделей, методів та систем оцінювання втрат від витоку персональних даних.....	99
<i>Пархоменко І.І.</i> Принципи побудови захищених каналів передачі конфіденційної інформації в умовах динамічного середовища.....	108
<i>Прокопович-Ткаченко Д.І., Бушков В.Г., Хрушков Б.С., Черкаський О.В., Козаченко І.М., Білан М.В.</i> Інтелектуальна модель прогнозування та реагування на кіберзагрози з використанням багатошарових рекурентних нейронних мереж і сучасних стратегій управління ризиками.....	116
<i>Прокопович-Ткаченко Д.І., Зверев В.П., Бушков В.Г., Козаченко І.М., Черкаський О.В.</i> Системні ризики цифрового аутсорсингу у державному секторі: аналіз вразливостей моделі “цифрового ескорту”.....	127
<i>Рзаєва С.Л., Складанний П.М., Машикіна І.В., Костюк Ю.В.</i> Модель реалізації керування доступом на основі ролей (RBAC) у багаторівневій архітектурі сховища даних.....	137

<i>Тимохін Ю.А.</i> Виявлення в реальному часі шахрайства в обході інтерконекту в телекомунікаційних мережах: підхід з низьким кодом camel framework та адаптація AI/ML.....	150
<i>Савченко В.А, Хавер А.В.</i> Оцінка впливу програмних інструментів на основі технологій штучного інтелекту на ресурсну ефективність щодо проведення деструктивних кібероперацій по відношенню до об'єктів критичної інфраструктури.....	165
<i>Чепель Д.О., Малахов С.В.</i> Багатобазовий хмарний моніторинг трафіку DNS для оперативної корекції поточних параметрів RPZ.....	176
<i>Шульга В.П., Іванченко І.С., Рижаков М.М.</i> Математична модель семантичної атрибуції кіберінцидентів у системах виявлення аномалій на основі глибокого навчання.....	186
<i>Верлань А.А., Жихай Ван, Чен Чен.</i> Моделювання забезпечення якості програмного забезпечення інтелектуального управління енергією на основі ШІ.....	199
<i>Шульга В.П., Корченко О.Г., Іванченко Є.В., Казмірчук С.В., Кондратюк С.В.</i> Критерії стратегічного оцінювання кібербезпеки держави: кібердипломатичний аспект.....	205
<i>Хохлачова Ю.Є., Флоров С.В., Черкаський О.В., Черкаський Д.О., Переметчик Д.О., Білан М.В.</i> Моделювання нейровірусних кампаній у мережевому трафіку на основі поєднання потокових, журнальних і байтових ознак.....	219
<i>Побережний В.О., Опірський І.Р.</i> Дослідження швидкодії методу передачі повідомлень із застосуванням OFF-CHAIN обробки даних для забезпечення цілісності та незмінності даних.....	230
Відомості про авторів.....	243
Анотації.....	245
Правила оформлення статей.....	253

CONTENT

<i>Bushkov V.H.</i> Modeling the Resilience of Electronic Communications to Hybrid Cyber Attacks: Approaches and Scenario Analysis of Infrastructure Resilience.....	8
<i>Haydur H.I., Hamza D.E.</i> A hybrid method for detecting malicious activity based on a stacking ensemble of classifiers.....	20
<i>Gapon A. O.</i> Experimental research, software implementation and evaluation of the effectiveness of the application of the software protection method based on hybrid analysis...	27
<i>Honcharov M.O., Narezhnii O.P., Malakhov S.V.</i> Analysis of prerequisites for ensuring resource consensus when performing steganographic data insertion procedures.....	37
<i>Deineka O.R., Harasymchuk O.I.</i> Agile approach to the implementation of the methodology of data collection, processing, storage and classification in accordance with SOC2 Type2 requirements.....	48
<i>Domarev V.V., Prokopovych-Tkachenko D.I., Zverev V.P., Bushkov V.G., Kozachenko I.M.</i> Situation-oriented security management systems based on a unified matrix model: a logical-linguistic and interdisciplinary approach.....	56
<i>Zhuravel Yu.I., Onyshko V.R.</i> Increasing the efficiency of the steganographic system through the use of image processing methods.....	68
<i>Ivanochko T. A., Semenyuk S. A.</i> Cybersecurity risk management using NIST CSF 2.0.....	75
<i>Laptev O.A., Stetsenko V.O.</i> The method of constructing a netherwriter cryptosystem based on M-codes.....	83
<i>Legominova S.V., Kapelyushna T.V., Shchavinskyi Yu.V., Muzhanova T.M.</i> Conceptual approaches to the integration of ethical norms into information security policy.....	90
<i>Lozova I.L., Rizak M.V., Khokhlachova Yu.E., Kotyk O.V.</i> Analysis of models, methods and systems for estimating losses from personal data leakage.....	99
<i>Parkhomenko I.I.</i> Principles of construction of secure channels for transmission of confidential information in a dynamic environment.....	108
<i>Prokopovych-Tkachenko D.I., Bushkov V.G., Khrushkov B.S., Cherkaskyi O.V., Kozachenko I.M., Bilan M.V.</i> An intelligent model for predicting and responding to cyber threats using multilayer recurrent neural networks and modern risk management strategies.....	116
<i>Prokopovych-Tkachenko D.I., Zverev V.P., Bushkov V.G., Kozachenko I.M., Cherkaskyi O.V.</i> Systemic risks of digital outsourcing in the public sector: analysis of vulnerabilities of the "digital escort" model.....	127
<i>Rzaeva S.L., Skladanniy P.M., Mashkina I.V., Kostyuk Yu.V.</i> A model for implementing role-based access control (RBAC) in a tiered data warehouse architecture.....	137
<i>Tymokhin Yu.A.</i> Real-Time Detection of Interconnect Bypass Fraud in Telecommunication Networks: CAMEL framework Low-Code Approach and AI/ML Adaptation.....	150

<i>Savchenko V.A., Khaver A.V.</i> Assessment of the impact of software tools based on artificial intelligence technologies on resource efficiency in conducting destructive cyber operations against critical infrastructure objects.....	165
<i>Chepel D. O., Malakhov S. V.</i> Multibased cloud monitoring of DNS traffic for operative correction of current RPZ parameters.....	176
<i>Shulga V.P., Ivanchenko I.S., Ryzhakov M.M.</i> Mathematical model of semantic attribution of cyber incidents in anomaly detection systems based on deep learning.....	186
<i>Verlan A.A., Zhi Hai Wang, Chen Chen.</i> Modelling the quality assurance of AI-based intelligent energy management software.....	199
<i>Shulga V.P., Korchenko O.H., Ivanchenko E.V., Kazmirchuk S.V., Kondratyuk S.V.</i> Criteria for strategic assessment of state cyber security: cyber diplomatic aspect.....	205
<i>Khokhlachova Yu.Ye., Florov S.V., Cherkaskyi O.V., Cherkaskyi D.O., Peremetchik D.O., Bilan M.V.</i> Modeling neurovirus campaigns in network traffic based on a combination of stream, log and byte features.....	219
<i>Poberezhnyk V.O., Opirskiy I.R.</i> Study of the speed of the message transmission method using OFF-CHAIN data processing to ensure data integrity and immutability.....	230
Authors profiles.....	243
Abstracts.....	245
Submission guidelines.....	253