

ЗМІСТ

<i>Борисенко І.І.</i> Проблема вибору контейнера для забезпечення стійкості стега до збурних дій.....	8
<i>Гашко А.О, Ананченко О.Є.</i> Графові нейронні мережі для протидії відмиванню коштів у кросчейн-блокчейн середовищах.....	14
<i>Дарієнко Д.Г., Козут Н.М.</i> Розробка методу вибору IDP провайдера для інтеграції з Docker.....	21
<i>Десятко А.М., Нікітенко Є.В., Гладких В.М.</i> Аналіз цифрових слідів та IoT-поведінкових даних у Smart-кампусі.....	31
<i>Єлісєєва Г.С.</i> Постквантова криптографія: сучасний стан та перспективи.....	38
<i>Іванченко Є.В., Ковальчук О.А.</i> Аналіз методик та стандартів управління кіберстійкістю інформаційних ресурсів.....	46
<i>Собчук А.В., Лаптева Т.О., Капустян Д.О., Степанченко Б.С., Лаптев С.О.</i> Метод оптимізації системи захисту об'єктів критичної інфраструктури за зваженої суми критеріїв.....	54
<i>Лаптев О.А., Браїловський М.М., Хорошко Г.О.</i> Авторське право у цифровому просторі ЄС в контексті кібербезпеки.....	61
<i>Макарчук А.В.</i> Метод аналізу залежності між частотою дискретизації сигналу та її апроксимацією з використанням інтерполяційних аналогів.....	68
<i>Хохлачова Ю.Є., Хавікова Ю. І., Щитов Д. М., Щитов О. М., Переметчик Д.О.</i> Оцінювання ефективності реінжинірингу цифрових державних послуг: методика, показники, результати.....	75
<i>Прокопович-Ткаченко Д.І., Єжихін А.В., Бушков В.Г., Черкаський О.В., Черкаський Д.О.</i> Формування цільового цифрового профілю безпеки мереж електронних комунікацій в умовах гібридних кібератак: ризик-орієнтований та багатокритеріальний підхід.....	87
<i>Костюк Ю.В., Складанний П.М.</i> Криптографічна модель довіри до подій безпеки в SIEM для інтелектуального формування мережевих інцидентів.....	103
<i>Хворостяний Р.В.</i> Мультиагентна модель управління кібербезпекою транспортної телекомунікаційної мережі.....	119
<i>Хвостенко В.С.</i> Еволюція смарт-контрактів у Web3- та DeFi-системах: архітектурна трансформація загроз безпеки та перспективи комплексного захисту.....	132
<i>Шуклін Г.В., Наконечний В.С., Данилов І.Д., Пена Ю.В.</i> Моделювання процесів виявлення технічних засобів несанкціонованого отримання інформації в умовах навмисного впливу завад за допомогою відстані Кульбака-Лейблера.....	142
<i>Яковенко В.О., Мормуль М.Ф.</i> Проектування кіберзахисту електронних сервісів у процесі реінжинірингу: нульова довіра, подієва аналітика та детекція прошивкових і мережевих атак методами глибокого навчання.....	149

<i>Синявський О.Ю.</i> Метод розрахунку чутливості каналу зв'язку БПЛА як критерію синтезу сигналів управління.....	163
<i>Колодюк А.В., Аронов А.О.</i> Аналітична модель впливу паралелізму на продуктивність системи впорядкованої доставки подій з At-Least-Once семантикою.....	169
Відомості про авторів.....	180
Анотації.....	182
Правила оформлення статей.....	189

CONTENT

<i>Borysenko I.I.</i> The problem of choosing a container to ensure the stability of stego to turbulent actions.....	8
<i>Hashko A.O., Ananchenko O.E.</i> Graph neural networks for anti-money laundering in cross-blockchain environments.....	14
<i>Darienko D.H., Kohut N.M.</i> Development of a method for selecting an IDP provider for integration with Docker.....	21
<i>Desyatko A.M., Nikitenko Ye.V., Gladkykh V.M.</i> Analysis of digital footprints and IoT behavioral data in the Smart Campus.....	31
<i>Yeliseeva H.S.</i> Post-quantum cryptography: current state and prospects.....	38
<i>Ivanchenko Ye.V., Kovalchuk O.A.</i> Analysis of methods and standards for managing cyber resilience of information resources.....	46
<i>Sobchuk A.V., Laptieva T.O., Kapustyan D.O., Stepanchenko B.S., Laptiev S.O.</i> Method for optimizing the protection system of critical infrastructure facilities using a weighted sum of criteria.....	54
<i>Laptiev O.A., Brailovskyi M.M., Khoroshko H.O.</i> Copyright in the EU digital space in the context of cybersecurity.....	61
<i>Makarchuk A.V.</i> A method of analysis of dependence between sampling rate of signal and its approximation using interpolation analogues.....	68
<i>Khokhlachova Yu.Ye., Khavikova Yu.I., Shchytyov D.M., Shchytyov O.M., Peremetchyk D.O.</i> Evaluating the effectiveness of reengineering digital public services: methodology, indicators, results.....	75
<i>Prokopovych-Tkachenko D.I., Ezhikhin A.V., Bushkov V.H., Cherkasky O.V., Cherkasky D.O.</i> Formation of a targeted digital security profile of electronic communications networks in the context of hybrid cyberattacks: a risk-based and multi-criteria approach.....	87
<i>Kostyuk Yu.V., Skladannyi P.M.</i> Cryptographic trust model for security events in SIEM for intelligent network incident generation.....	103
<i>Hvorostyanyi R.V.</i> Multi-agent model for managing cybersecurity of a transport telecommunications network.....	119
<i>Khvostenko V.S.</i> The evolution of smart contracts in Web3 and DeFi systems: architectural transformation of security threats and prospects for comprehensive protection.....	132
<i>Shuklin H.V., Nakonechny V.S., Danylov I.D., Pepa Yu.V.</i> Modeling the processes of detecting technical means of unauthorized information acquisition under conditions of intentional interference using the Kullback-Leibler distance.....	142
<i>Yakovenko V.O., Mormul M.F.</i> Designing cyber defense of electronic services in the reengineering process: zero trust, event analytics, and detection of firmware and network attacks using deep learning methods.....	149

<i>Sinyavsky O.Yu.</i> Method for calculating the sensitivity of the UAV communication channel as a criterion for synthesizing control signals.....	163
<i>Kolodyuk A.V., Aronov A.O.</i> Analytical model of the impact of parallelism on the performance of an ordered event delivery system with At-Least-Once semantics.....	169
Authors profiles.....	180
Abstracts.....	182
Submission guidelines.....	189