Kasmin D. Algorithmic means of ensuring network security and websites: trends, models, future cases / G. Bekmagambetova, A. Polukhin, V. Evdokimov, D. Kasmin, O. Dmytriienko // Amazonia Investiga. – 2023. – 12(65). – P. 149–163.

– [Електронний ресурс] – Режим доступу: https://doi.org/10.34069/AI/2023.65.05.15

Касьмін Д. С.

Алгоритмічні засоби забезпечення мережевої безпеки та веб-сайтів : тренди, моделі, кейси майбутнього

Kasmin D. S.

Algorithmic means of ensuring network security and websites: trends, models, future cases

Анотація

Мета дослідження ? встановлення ймовірних трендів розвитку алгоритмічних засобів мережної безпеки та захисту веб-ресурсів у майбутньому. У якості методів дослідження в даній публікації використаний бібліометричний аналіз 500 релевантних публікацій, що дозволив встановити ймовірні тренди майбутнього розвитку предметного поля. За результатами дослідження встановлено, що наразі найбільш ймовірними алгоритмічними засобами мережної безпеки та захисту веб-сайтів, що отримають інтенсивний розвиток у майбутньому є технології блокчейну (для захисту міжресурсного контакту), глибинного та машинного навчання (для аналізу та виявлення атак та цифрових аномалій), штучного інтелекту та нейромереж (для розробки складних безпекових алгоритмів), а також предиктивного аналізу (для попередження ймовірних атак та ін'єкцій шкідливих даних). Разом з тим, технологічний розвиток дозволяє визначити альтернативні безпекові засоби, серед яких квантова та пост квантова криптографія (що є можливою внаслідок розвитку квантового обчислення), розширена реальність (що є наступною ітерацією розвитку інтерфейсу машинолюдської взаємодії), біометрична ідентифікація (що є наступною ітерацією систем автентифікації та розпізнання) та DevSecOps (що є перспективною технологією виробництва цифрових засобів і систем, що мають відносно нижчий рівень вразливостей до відомих цифрових загроз). Встановлений корелятивний вплив технологій та рішень Industry 4.0 на досліджувані аспекти безпекового сектору Всемережжя. Зростання мережі пристроїв вимагає вдосконалення безпекових алгоритмів в парадигмі технологій Industry 4.0, що дозволять ефективніше виявляти та запобігати кібератакам та

захищати дані користувачів.

Ключові слова: штучний інтелект, нейромережі, машинне навчання, квантова криптографія, Industry 4.0.

Анотація

The purpose of the study is to establish probable trends in the development of algorithmic means of network security and the protection of web resources in the future. The research methods used in this

publication are a bibliometric analysis of 500 relevant publications, which allowed us to establish probable trends in the future development of the subject field. The study found that currently the most likely algorithmic means of network security and website protection that will be intensively developed in the future are blockchain technologies (to protect inter-resource contact), deep and machine learning (to analyze and detect attacks and digital anomalies), artificial intelligence and neural networks (to develop complex security algorithms), and predictive analysis (to prevent possible attacks and malicious data injections). At the same time, technological development makes it possible to identify alternative security tools, including quantum and post-quantum cryptography (which is possible due to the development of quantum computing), augmented reality (which is the next iteration of the development of the interface between machine-human interaction), biometric identification (which is the next iteration of authentication and recognition systems) and DevSecOps (which is a promising technology for the production of digital tools and systems that have a relatively lower level of vulnerability to known digital threats). The correlative impact of Industry 4.0 technologies and solutions on the studied aspects of the security sector of the World Wide Web has been established. The growth of the network of devices requires the improvement of security algorithms in the paradigm of Industry 4.0 technologies, which will allow more effective detection and prevention of cyberattacks and protection of user data.

Ключові слова: штучний інтелект, нейромережі, машинне навчання, квантова криптографія, Industry 4.0

Keywords: artificial intelligence, neural networks, machine learning, quantum cryptography, Industry 4.0.