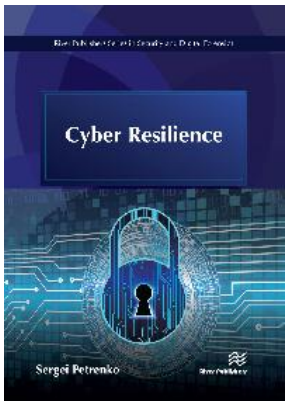

River Publishers Series in Digital Security and Forensics

Cyber Resilience

Author: Sergei Petrenko, Innopolis University, Russia
ISBN: 9788770221160
e-ISBN: 9788770221153
Available From: October 2019
Price: € 95.00

Description:

Modern cyber systems acquire more emergent system properties, as far as their complexity increases: cyber resilience, controllability, self-organization, proactive cyber security and adaptability. Each of the listed properties is the subject of the cybernetics research and each subsequent feature makes sense only if there is a previous one.

Cyber resilience is the most important feature of any cyber system, especially during the transition to the sixth technological stage and related Industry 4.0 technologies: Artificial Intelligence (AI), Cloud and foggy computing, 5G +, IoT/IIoT, Big Data and ETL, Q-computing, Blockchain, VR/AR, etc. We should even consider the cyber resilience as a primary one, because the mentioned systems cannot exist without it. Indeed, without the sustainable formation made of the interconnected components of the critical information infrastructure, it does not make sense to discuss the existence of 4.0 Industry cyber-systems. In case when the cyber security of these systems is mainly focused on the assessment of the incidents' probability and prevention of possible security threats, the cyber resilience is mainly aimed at preserving the targeted behavior and cyber systems' performance under the conditions of known (about 45 %) as well as unknown (the remaining 55 %) cyber attacks.

This monograph shows that modern Industry 4.0. Cyber systems do not have the required cyber resilience for targeted performance under heterogeneous mass intruder cyber-attacks. The main reasons include a high cyber system structural and functional complexity, a potential danger of existing vulnerabilities and "sleep" hardware and software tabs, as well as an inadequate efficiency of modern models, methods, and tools to ensure cyber security, reliability, response and recovery. A new formulation of the cyber resilience problem under heterogeneous mass cyber-attacks is proposed, in which the cyber system performance recovery in destructive software impacts prevents significant or catastrophic consequences. Here, the idea of ensuring the cyber resilience is to give the cyber systems the ability to develop immunity to disturbances of the computational processes under destructive influences, by analogy with the immune system protecting a living organism.

The book contains three chapters, devoted to the following topics:

- Development of the Cyber Resilience Management Concept of modern technological platforms and cyber-systems of 4.0 Industry;
- Development of a corporate cyber risk management methodology;
- Technical implementation of the corporate program of business sustainability management based on the best practices (standards).

Keywords: Cyber Systems of 4.0 Industry, Cyber Resilience Management Concept, Quantitative Metrics and Cyber Resistance measures, Cyber Resiliency Engineering Framework, Business continuity management.