

**Prof. Dr. Igor V. Kotenko**

St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS), St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences, St. Petersburg, Russia.

**TITLE**

Intelligent Situational Awareness for Cyber Security

**ABSTRACT**

Main aspects of intelligent situation awareness in the area of cyber security are considered. The talk concerns different aspects of cyber situation awareness, including situation perception, impact assessment, situation tracking, projecting future possible actions, understanding of adversary and countermeasures selection. Models, techniques and tools for advanced intelligent cyber situation awareness are analyzed. They are based on big data analytics, artificial intelligence, machine learning, user and application behavior analytics and interactive visualization. Examples of research applications and developed intelligent components for intrusion detection, security monitoring and incident management are demonstrated.

**SHORT BIO**

Igor V. Kotenko is a Chief Scientist and Head of Research Laboratory of Computer Security Problems of the St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS). He is also Professor of the Information Technologies, Mechanics and Optics University and the Bonch-Bruевич Saint Petersburg State University of Telecommunications.

He is the author of more than 500 refereed publications, including 13 books and monographs. Main research results are in artificial intelligence, telecommunication, cyber security, including network intrusion detection, modeling and simulation of network attacks, vulnerability assessment, security information and event management, verification and validation of security policy.

Igor V. Kotenko is a laureate of the St. Petersburg Government award for outstanding scientific achievements in the field of science and technology. He was a project leader in the research projects from the US Air Force research department, via its EOARD (European Office of Aerospace Research and Development) branch, EU FP7 and FP6 Projects, HP, Intel, F-Secure, Huawei, etc. The research results of Igor Kotenko were tested and implemented in multitude of Russian research and development projects, including grants of the Russian Foundation of Basic Research, Russian Science Foundation and State contracts. He has been an invited speaker on multitude of international conferences and has chaired several international conferences.

