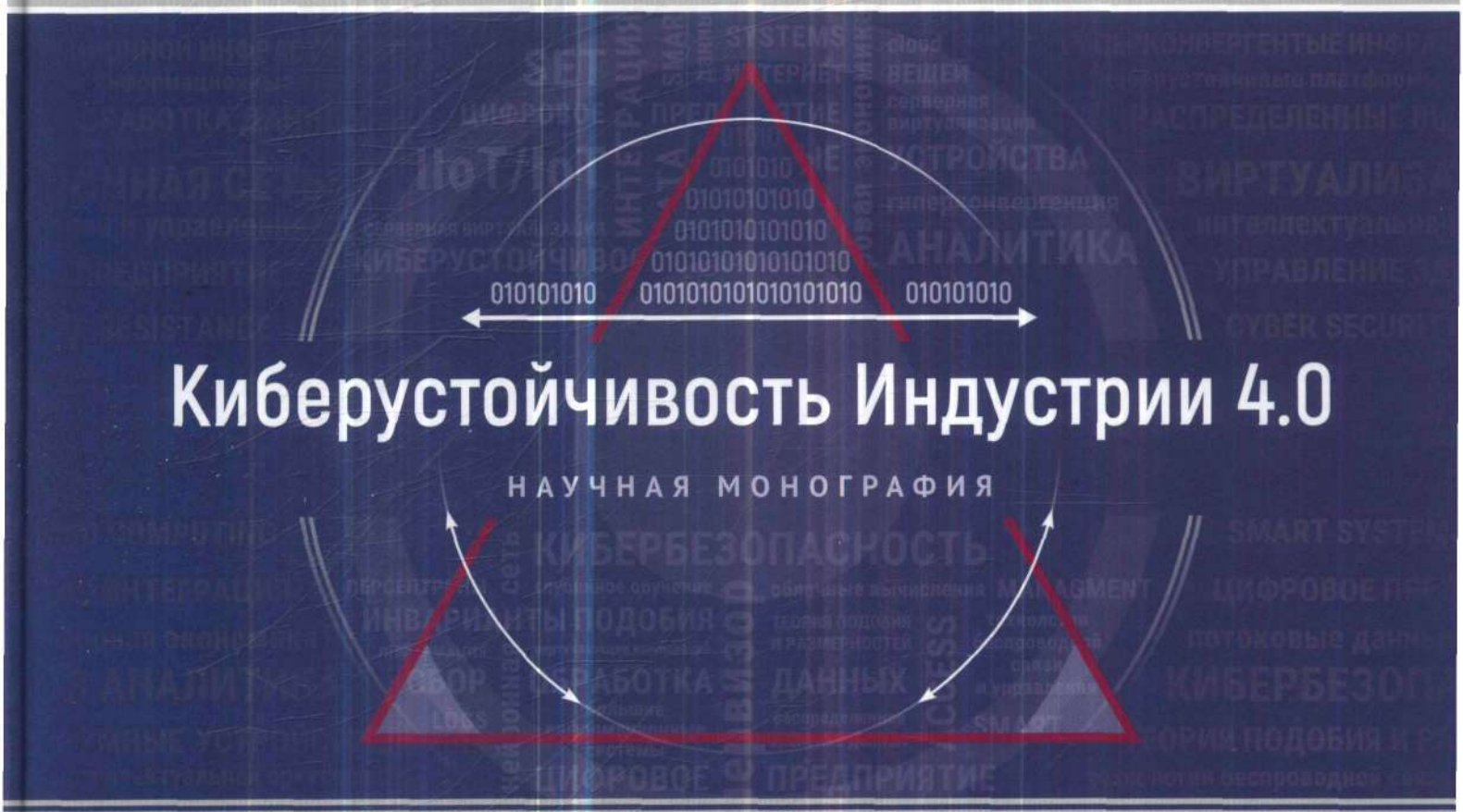
Иннополис Университи МФТИ

Сергей Петренко



Киберустойчивость Индустрии 4.0

НАУЧНАЯ МОНОГРАФИЯ

Афина Издательский дом

ООО «Издательский Дом «Афина», 194017, Санкт-Петербург, пр. Тореза, д. 98, корп. 1, тел./факс: (812) 347-74-12,
e-mail: magazine@inside-zi.ru, www.inside-zi.ru

2020

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Московский физико-технический институт
(национальный исследовательский университет)

Автономная некоммерческая организация высшего образования
«Университет Иннополис»

С. А. Петренко

КИБЕРУСТОЙЧИВОСТЬ ИНДУСТРИИ 4.0

Научная монография

«Издательский Дом «Афина»

Санкт-Петербург
2020

УДК 004.56
ББК 32.972.14
П71

Издание осуществлено при финансовой поддержке
Российского фонда фундаментальных исследований по проекту № 20-17-00005, не подлежит продаже

Рецензенты:

Заслуженный деятель науки Российской Федерации, доктор технических наук, профессор, профессор кафедры «Системы сбора и обработки информации» ВКА им. А. Ф. Можайского
Ломако Александр Григорьевич

Член Экспертного совета при Правительстве Российской Федерации, доктор технических наук, CISSP (ISC)², профессор кафедры ИУ8 «Информационная безопасность» МГТУ им. Н. Э. Баумана
Марков Алексей Сергеевич

Петренко С. А.
П71 Киберустойчивость Индустрии 4.0: научная монография / Петренко С. А. – СПб: «Издательский Дом «Афина», 2020. – 256 с.

ISBN 978-5-6045272-0-7

Киберустойчивость (англ. – *Cyber Resilience*) является важнейшим свойством любой киберсистемы, особенно в условиях перехода на шестой технологический уклад и сопутствующие технологии *Индустрии 4.0*: *Artificial Intelligence (AI), Cloud and foggy computing, 5G+, IoT/IIoT, Big Data и ETL, Q-computing, Blockchain, VR/AR* и пр. Можно даже считать его первичным, так как без него упомянутые системы как таковые не могут существовать.

В настоящей монографии показано, что современные киберсистемы *Индустрии 4.0* не обладают требуемой *киберустойчивостью* для целевого функционирования в условиях *разнородно-массовых кибератак* злоумышленников. Основными причинами этого являются высокая структурная и функциональная сложность киберсистем, потенциальная опасность имеющихся *уязвимостей* и *«спящих» аппаратно-программных закладок*, а также недостаточная эффективность известных моделей, методов и средств обеспечения кибербезопасности (англ. – *Cyber Security*), надежности (англ. – *Reliability*) и отказоустойчивости (англ. – *Response and Recovery*). Предложена новая постановка задачи обеспечения *киберустойчивости* в условиях разнородно-массовых кибератак, в которой организация восстановления функционирования киберсистем в ходе деструктивных программных воздействий упреждает приведение к существенным или катастрофическим последствиям. Замысел обеспечения киберустойчивости здесь заключается в придании киберсистемам способности вырабатывать *иммунитет* к возмущениям процессов вычислений в условиях деструктивных воздействий по аналогии с *иммунной системой* защиты живого организма.

В монографии представлено возможное решение научной проблемы *организации работы критически важной информационной инфраструктуры Индустрии 4.0 с требуемой киберустойчивостью в условиях ранее неизвестных разнородно-массовых кибератак злоумышленников на основе инвариантов подобия*. Эта монография является первой работой по упомянутой проблеме. При этом она содержит результаты не только *качественного*, но и *количественного* изучения киберустойчивости, что позволило впервые открыть предельный *закон эффективности* обеспечения киберустойчивости киберсистем *Индустрии 4.0*. По этой причине монография представляет несомненный теоретический и практический интерес для специалистов в области кибернетики, киберустойчивости и информационной безопасности.

ISBN 978-5-6045272-0-7

УДК 004.56
ББК 32.972.14

MINISTRY OF SCIENCE AND HIGHER EDUCATION OF THE RUSSIAN FEDERATION

Moscow Institute of Physics and Technology
(National Research University)

Innopolis University

S. A. Petrenko

CYBER RESILIENCE INDUSTRY 4.0

The scientific monograph

Publishing House Afina

St. Petersburg
2020

UDC 004.56
LBC 32.972.14
P71

The reported study was funded by RFBR, project number 20-17-00005

Reviewers:

Mozhaisky Military Space Academy,
Department of the Systems for Data Collection and Processing, Professor,
Doctor of Technical Sciences, Professor
A. G. Lomako

Bauman Moscow State Technical University, National research university of technology,
Department IC8 «Information Security»,
Dr. Sc. (Comp.), Associate Professor, CISSP
A. S. Markov

S. A. Petrenko
P71 Cyber Resilience Industry 4.0: The scientific monograph / S. A. Petrenko – St. Petersburg: Publishing House Afina, 2020. – 256 p.

ISBN 978-5-6045272-0-7

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. 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 key research results on the scientific problem of *cyber resilience of critical information infrastructure in the previously unknown heterogeneous mass intruder cyber-attacks based on similarity invariants* are presented. It is essential that the obtained results significantly complement the well-known practices and recommendations of *ISO 22301, MITRE PR 15-1334* and *NIST SP 800-160* in terms of developing *quantitative metrics and cyber resistance measures.* This makes it possible for the first time to discover and formally present the *ultimate efficiency law of cyber resilience of modern Industry 4.0 systems under increasing security threats.* For this reason, the monograph performs the undoubted theoretical and practical interest for cybernetics, cyber resilience and information security specialists.

UDC 004.56
LBC 32.972.14

Содержание

Издание осуществлено при финансовой поддержке
Российского фонда фундаментальных исследований по проекту № 20-17-00005,
не подлежит продаже

Киберустойчивость (англ. – *Cyber Resilience*) является важнейшим свойством любой киберсистемы, особенно в условиях перехода на шестой технологический уклад и сопутствующие технологии *Индустрии 4.0: Artificial Intelligence (AI), Cloud and foggy computing, 5G+, IoT/IIoT, Big Data и ETL, Q-computing, Blockchain, VR/AR* и пр. Можно даже считать его первичным, так как без него упомянутые системы как таковые не могут существовать.

В настоящей монографии показано, что современные киберсистемы *Индустрии 4.0* не обладают требуемой *киберустойчивостью* для целевого функционирования в условиях *разнородно-массовых кибератак* злоумышленников. Основными причинами этого являются высокая структурная и функциональная сложность киберсистем, потенциальная опасность имеющихся *уязвимостей* и *«спящих» аппаратно-программных закладок*, а также недостаточная эффективность известных моделей, методов и средств обеспечения кибербезопасности (англ. – *Cyber Security*), надежности (англ. – *Reliability*) и отказоустойчивости (англ. – *Response and Recovery*). Предложена новая постановка задачи обеспечения *киберустойчивости* в условиях разнородно-массовых кибератак, в которой организация восстановления функционирования киберсистем в ходе деструктивных программных воздействий упреждает приведение к существенным или катастрофическим последствиям. Замысел обеспечения киберустойчивости здесь заключается в придании киберсистемам способности вырабатывать *иммунитет* к возмущениям процессов вычислений в условиях деструктивных воздействий по аналогии с *иммунной системой* защиты живого организма.

В монографии представлено возможное решение научной проблемы *организации работы критически важной информационной инфраструктуры Индустрии 4.0 с требуемой киберустойчивостью в условиях ранее неизвестных разнородно-массовых кибератак злоумышленников на основе инвариантов подобия*. Эта монография является первой работой по упомянутой проблеме. При этом она содержит результаты не только *качественного*, но и *количественного* изучения киберустойчивости, что позволило впервые открыть предельный *закон эффективности* обеспечения киберустойчивости киберсистем *Индустрии 4.0*. По этой причине монография представляет несомненный теоретический и практический интерес для специалистов в области кибернетики, киберустойчивости и информационной безопасности.

Сергей Петренко

Доктор технических наук, профессор, руководитель Центра информационной безопасности Университета Иннополис. Ведущий научный сотрудник Московского физико-технического института (Физтеха), Физтех-школы радиотехники и компьютерных технологий (ФРКТ), Лаборатории Космической Информатики. Конструктор 20 национальных центров мониторинга угроз информационной безопасности и реагирования на инциденты информационной безопасности CERT (Computer Emergency Response Team) и CSIRT (Computer Security Incident Response Team). Эксперт секции по проблемам информационной безопасности научного совета при Совете Безопасности Российской Федерации. Удостоен премии «Большой ЗУБР» и «Золотой ЗУБР» в 2014 году за национальные проекты Российской Федерации в области информационной безопасности.

ISBN 978-5-6045272-0-7