Безопасность и устойчивость цифровых экосистем и платформ

391 стр. PDF 2021 г.

Киберустойчивость (англ. – *Cyber Resilience*) является важнейшим свойством любой цифровой экосистемы или платформы, особенно в условиях перехода на VI технологический уклад и сопутствующие технологии *Индустрии 4.0: Artificial Intelligence (AI), Cloud and fog gycomputing, 5G+, IoT/IIoT, Big Data и ETL, Q-computing, Blockchain, VR/AR* и прочие. Можно даже считать его первичным, так как без него упомянутые киберсистемы не могут существовать. В настоящем пособии показано, что современные цифровые экосистемы и платформы не обладают требуемой киберустойчивостью для целевого функционирования в условиях разнородно-массовых кибератак злоумышленников. Основными причинами данного положения вещей являются высокая структурная и функциональная сложность этих систем, 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 по обеспечению киберустойчивости в современных условиях, в которых организация восстановления функционирования цифровых экосистем и платформ в ходе деструктивных программных воздействий упреждает приведение к существенным или катастрофическим последствиям. Замысел обеспечения киберустойчивости здесь заключается в придании упомянутым системам способности вырабатывать иммунитет к возмущениям процессов вычислений в условиях деструктивных воздействий – по аналогии с иммунной системой живого организма. В пособии изложено возможное решение научной проблемы обеспечения киберустойчивости экосистем и платформ *в условиях роста угроз безопасности – на основе авторских моделей и методов самовосстановления, а также подобия вычислений, искусственного интеллекта и иммунной защиты, доверенной среды облачных вычислений, безопасного Интернета вещей (IIoT/IoT), сбора и обработки больших данных (Big Data и ETL), квантового криптоанализа (Q-computing) и др.*

Пособие содержит результаты не только качественного, но и количественного изучения киберустойчивости цифровых экосистем и платформ государства и бизнеса, поэтому представляет несомненный теоретический и практический интерес для специалистов в области цифровой экономики, компьютерных технологий и кибербезопасности.