

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 computing, 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.

Введение

Глава 1. Актуальность проблемы обеспечения киберустойчивости цифровых экосистем и платформ в условиях роста угроз безопасности

- 1.1. Ландшафт угроз кибербезопасности
 - 1.1.1. Известные приемы злоумышленников
 - 1.1.2. Угрозы кибербезопасности АСУ ТП
- 1.2. Понятие «непрерывности бизнеса»
 - 1.2.1. Корпоративная программа ЕСР
 - 1.2.2. Состав и структура программы ЕСР
- 1.3. Предельные возможности технологий отказоустойчивости и аварийного восстановления
 - 1.3.1. Общие подходы и направления
 - 1.3.2. Инфраструктурные решения
- 1.4. Новая постановка задачи по обеспечению киберустойчивости
 - 1.4.1. Имеющийся научно-технический задел
 - 1.4.2. Концепция киберустойчивости цифровых экосистем и платформ

Глава 2. Модели и методы управления киберрисками

- 2.1. Практика управления киберрисками
 - 2.1.1. Эволюция управления киберрисками
 - 2.1.2. Возможные методические рекомендации
 - 2.1.3. Методы получения субъективной вероятности
- 2.2. Развитие метрик киберустойчивости
 - 2.2.1. Возможная метрика киберустойчивости
 - 2.2.2. Задание предикатных функций
 - 2.2.3. Верификация схем программ
- 2.3. Примеры управления киберрисками
 - 2.3.1. Пример методики управления киберрисками
 - 2.3.2. Пример BIA (Business Impact Analysis)
 - 2.3.3. Инструментальные средства управления киберрисками

Глава 3. Непрерывность бизнеса как ключевой компонент устойчивости цифровых экосистем и платформ

- 3.1. Лучшая практика управления непрерывностью бизнеса**
 - 3.1.1. Международный стандарт ISO 22301:2019
 - 3.1.2. Практика института BCI
 - 3.1.3. Практика института DRI
 - 3.1.4. Рекомендации института SANS
- 3.2. Лучшая практика управления информационными рисками**
 - 3.2.1. Семейство стандартов ISO 31000
 - 3.2.2. Известные стандарты управления рисками
 - 3.2.3. Стандарт NIST SP 800-30
 - 3.2.4. Методология OCTAVE
 - 3.2.5. Жизненный цикл MG-2
 - 3.2.6. Стандарт COBIT 2019
 - 3.2.7. Модель зрелости SA-CMM
- 3.3. Лучшая практика управления непрерывностью ИТ**
 - 3.3.1. Стандарт COBIT 2019
 - 3.3.2. Библиотека ITIL V4
- 3.4. Лучшая практика управления информационной безопасностью и непрерывностью бизнеса**
 - 3.4.1. Стандарты ISO/IEC 27001:2013 и ISO/IEC 27031:2011
 - 3.4.2. Разработка и внедрение плана BCP
 - 3.4.3. Набор практик RESILIA 201

Глава 4. Оценка зарубежного опыта

- 4.1. Лучшая практика консультантов**
 - 4.1.1. Типовые услуги в области BCM
 - 4.1.2. Оценки RA и BIA
 - 4.1.3. Определение стратегии BC
 - 4.1.4. Улучшение стратегии BC
- 4.2. Лучшая практика производителей гиперконвергентных платформ**
 - 4.2.1. Методы выполнения работ
 - 4.2.2. Подход команды IBM BCRS
 - 4.2.3. Услуги команды IBM BCRS
 - 4.2.4. Пример выбора решения
 - 4.2.5. Пример постановки задачи
- 4.3. Лучшая практика производителей системного программного обеспечения**
 - 4.3.1. Характеристика подхода BCM
 - 4.3.2. Описание функции ITCM

Глава 5. Разработка новых технологий для обеспечения киберустойчивости цифровых экосистем и платформ

- 5.1. Самовосстанавливающиеся облачные вычисления**
 - 5.1.1. Выбор и обоснование инструментальной платформы
 - 5.1.2. Состав и структура устойчивого частного облака
- 5.2. Самовосстанавливающиеся тракты передачи данных Интернета вещей**
 - 5.2.1. Критический анализ известных платформ IIoT/IoT
 - 5.2.2. Обоснование подхода к построению киберустойчивых платформ IIoT/IoT
- 5.3. Программно-определяемое хранение данных**
 - 5.3.1. Известные системы хранения данных
 - 5.3.2. Преимущества SDS-решений
 - 5.3.3. Достоинства кластерных SDS-решений
- 5.4. Иммунная защита цифровых экосистем и платформ**
 - 5.4.1. Потенциальные возможности искусственных иммунных систем
 - 5.4.2. Обеспечение киберустойчивости на основе кибериммунитета

Заключение

Литература