Оглавление

Вводное слово ректора Университета Иннополис А. Г. Тормасова 6

Вводное слово заместителя генерального директора SAP СНГ Д. А. Шепелявого 11

Введение 15

Глава 1. Актуальность проблемы обеспечения киберустойчивости Цифровой экономики Российской Федерации в условиях роста угроз безопасности 24

1.1. Ландшафт угроз кибербезопасности 24

1.1.1. Известные приемы злоумышленников 25

1.1.2. Угрозы кибербезопасности АСУ ТП 37

1.2. Понятие «непрерывность бизнеса» 56

1.2.1. Корпоративная программа ECP 56

1.2.2. Состав и структура программы ECP 74

1.3. Предельные возможности технологий отказоустойчивости и аварийного восстановления 85

1.3.1. Общие подходы и направления 85

1.3.2. Инфраструктурные решения 93

1.4. Новая постановка задачи по обеспечению киберустойчивости 107

1.4.1. Имеющийся научно-технический задел 107

1.4.2. Концепция киберустойчивости цифровых экосистем и платформ 120

Глава 2. Непрерывность бизнеса как ключевая компонента устойчивости Цифровой экономики Российской Федерации 139

2.1. Лучшая практика управления непрерывностью бизнеса 140

2.1.1. Международный стандарт ISO 22301:2019 140

2.1.2. Практика института BCI 146
2.1.3. Практика института DRII 151
2.1.4. Рекомендации института SANS 155
2.2. Лучшая практика управления информационными рисками 175
2.2.1. Семейство стандартов ISO 31000 175
2.2.2. Известные стандарты управления рисками 178
2.2.3. Стандарт NIST SP 800-30 181
2.2.4. Методология OCTAVE 185
2.2.5. Жизненный цикл MG-2 186
2.2.6. Стандарт COBIT 2019 188
2.2.7. Модель зрелости SA-CMM 189
2.3. Лучшая практика управления непрерывностью ИТ 190
2.3.1. Стандарт COBIT 2019 190
2.3.2. Библиотека ITIL V4 193
2.4. Лучшая практика управления информационной безопасностью и непрерывностью бизнеса. 208
2.4.1. Стандарты ISO/IEC 27001:2013 и ISO/IEC 27031:2011. 208
2.4.2. Разработка и внедрение плана BCP 212
2.4.3. Набор практик RESILIA 2015 216

Глава 3. Оценка пригодности зарубежного опыта для обеспечения киберустойчивости Цифровой экономики Российской Федерации 220

3.1. Лучшая практика консультантов 221
3.1.1. Типовые услуги в области BCM 222
3.1.2. Оценки RA и BIA 225
3.1.3. Определение стратегии BC 232
3.1.4. Улучшение стратегии BC 240
3.2. Лучшая практика производителей гиперконвергентных платформ 245
3.2.1. Методы выполнения работ 246
3.2.2. Подход команды IBM BCRS 250

3.2.3. Услуги команды IBM BCRS 253
3.2.4. Пример выбора решения 266
3.2.5. Пример постановки задачи 277
3.3. Лучшая практика производителей системного программного обеспечения 284
3.3.1. Характеристика подхода BCM 285
3.3.2. Описание функции ITCM 290

Глава 4. Разработка новых технологий для обеспечения киберустойчивости Цифровой экономики Российской Федерации 293

4.1. Самовосстанавливающиеся облачные вычисления 294
4.1.1. Выбор и обоснование инструментальной платформы 294
4.1.2. Состав и структура устойчивого частного облака 298
4.2. Самовосстанавливающиеся тракты передачи данных Интернета вещей 308
4.2.1. Критический анализ известных платформ IIoT/IoT 308
4.2.2. Обоснование подхода к построению киберустойчивых платформ IIoT/IoT 320
4.3. Программно-определяемое хранение данных 329
4.3.1. Известные системы хранения данных 329
4.3.2. Преимущества SDS-решений 332
4.3.3. Достоинства кластерных SDS-решений 338
4.4. Иммунная защита цифровых экосистем и платформ 348
4.4.1. Потенциальные возможности искусственных иммунных систем 349
4.4.2. Обеспечение киберустойчивости на основе кибериммунитета 372

Заключение 380

Об авторе 384