

Содержание

Вводные слова	8
Введение	12
Глава 1. Актуальность научной проблемы придания современным киберфизическим системам кибериммунитета для упреждения катастрофических последствий кибератак	14
1.1. Рост угроз безопасности киберфизических систем	14
1.1.1. Основные приемы злоумышленников	14
1.1.2. Уязвимости «умных» устройств.....	19
1.1.3. Угрозы безопасности АСУ ТП	21
1.1.4. География кибератак на АСУ ТП	28
1.1.5. Усиление мер защиты в условиях COVID-19	29
1.2. Выбор биологической метафоры кибериммунитета	31
1.2.1. Основные понятия и определения иммунитета.....	32
1.2.2. Развитие модельных представлений об иммунитете.....	35
1.2.3. Еще более древняя организация иммунитета.....	41
1.2.4. Первые представления иммунитета в действии	45
1.3. Концепция иммунной защиты Индустрии 4.0	48
1.3.1. Концептуальная модель вычислений с иммунной памятью.....	49
1.3.2. Восстановление функциональных спецификаций приложений.....	51
1.3.3. Доказательство правильности функциональной семантики вычислений	52
1.3.4. Многомодельная организация вычислений с иммунной памятью	55
Глава 2. Оценка пригодности моделей и методов биологической иммунологии для создания достаточного математического базиса кибериммунологии.....	58
2.1. Математические модели биологической иммунологии.....	58
2.1.1. Модели вирусной динамики.....	58
2.1.2. Модели перекрестного связывания.....	60
2.1.3. Модели передачи сигналов	61
2.1.4. Модели idiotипических сетей	62
2.1.5. Модели «свой – чужой»	63
2.1.6. Многоагентные системы иммунной защиты	63
2.2. Известные модели иммунного ответа	64
2.2.1. Первые модели иммунного ответа.....	64
2.2.2. Современные представления иммунного ответа	65
2.2.3. Уравнения пролиферации и дифференцировки.....	67
2.2.4. Треугольник дифференцировки	69
2.3. Первые модели интеллектуальной кибербезопасности	69
2.3.1. Многоагентная модель противодействия кибератакам	70
2.3.2. Многоагентная модель обнаружения вторжений.....	71
2.3.3. Многоагентная модель противостояния в киберпространстве.....	73
2.4. Возможные модели обеспечения киберустойчивости	75
2.4.1. Основные понятия и определения киберустойчивости	75

2.4.2. Сопроблемы обеспечения киберустойчивости	78
2.4.3. Замысел разрешения проблемы киберустойчивости	79
2.4.4. Возможная методика «паспортизации» вычислений	80
2.4.5. Определения элементарного и сложного вычислений	81
2.4.6. Моделирование вычислений в условиях возмущений	85
Глава 3. Развитие систем обнаружения вторжений и аномалий на основе методов иммунного	
ответа для противодействия ранее неизвестным вредоносным программным воздействиям.....	90
3.1. Роль и место иммунных методов обнаружения вторжений	91
3.1.1. Общая классификация методов обнаружения вторжений и аномалий.....	91
3.1.2. Алгоритмы клональной селекции вредоносного программного кода	96
3.1.3. Комбинация иммунного и нейросетевого детекторов вредоносного кода.....	98
3.1.4. Оценка результативности методов обнаружения вторжений и аномалий	101
3.2. Улучшение метода иммунного ответа на вредоносный программный код	107
3.2.1. Постановка задачи на улучшение метода иммунного ответа.....	107
3.2.2. Основные идеи нового метода иммунного ответа на вторжения	110
3.2.3. Возможные алгоритмы обнаружения и обучения механизма иммунного ответ	112
3.3. Опытное внедрение новой системы иммунного ответа на вторжения	112
3.3.1. Описание стенда для натуральных испытаний	112
3.3.2. Основные алгоритмы фильтрации сетевого трафика.....	114
3.3.3. Оценка полученного эффекта	117
Глава 4. Определение предельных возможностей искусственных иммунных систем	
для самовосстановления киберфизических систем в условиях роста угроз безопасности	120
4.1. Направления развития искусственных иммунных систем.....	121
4.1.1. Развитие теории иммунных сетей Н. Эрне	121
4.1.2. Возможности известных алгоритмов иммунной защиты	123
4.1.3. Развитие моделей генерации иммунного ответа П. Матзингер	126
4.1.4. Возможности иммунокомпьютинга А. О. Тараканова	128
4.1.5. Особенности организации вычислений на иммунокомпьютерах.....	130
4.2. Усиление возможностей иммунных детекторов путем комплексирования.....	134
4.2.1. Снятие ограничений известных классификаторов кибератак	134
4.2.2. Возможная схема гибридизации классификаторов кибератак.....	136
4.2.3. Оценка эффективности гибридного классификатора кибератак.....	138
4.3. Возможные решения задачи обнаружения программных закладок	139
4.3.1. Постановка задачи обнаружения программных закладок	139
4.3.2. Возможные способы выявления дефектов программ	143
4.3.3. Методы выявления дефектов программ на основе сетей Петри.....	147
4.4. Возможные решения задачи восстановления функциональной	
семантики вычислений	151
4.4.1. Методы восстановительной коррекции программ.....	151
4.4.2. Метод «паспортизации» вычислений на основе размерностей	154
4.4.3. Возможная методика контроля целостности вычислений.....	162
4.4.4. Метод нейтрализации программных закладок.....	164
4.4.5. Конструирование автомата динамического контроля вычислений.....	169
Глава 5. Примеры разработки самовосстанавливающихся киберфизических систем	
с кибериммунитетом для упреждения катастрофических последствий кибератак.....	175
5.1. Возможные модели и методы самовосстановления на основе кибериммунита	176
5.1.1. Модель абстрактного вычислителя с иммунной памятью	176
5.1.2. Модели динамики вычислений в условиях возмущений.....	179
5.1.3. Метод контроля функциональной семантики вычислений	181

5.1.4. Метод синтеза абстрактных программ восстановления	184
5.2. Пример разработки самовосстанавливающегося частного облака	193
5.2.1. Выбор и обоснование инструментальных средств разработки.....	193
5.2.2. Состав и структура возможного частного облака с кибериммунитетом	195
5.2.3. Использование программно-определяемого хранилища данных Ceph	197
5.2.4. Применение сред управления контейнерами Docker и Kubernetes	198
5.3. Пример разработки самовосстанавливающегося Интернета вещей.....	200
5.3.1. Ограничения известных платформ Интернета вещей	200
5.3.2. Выбор платформы Интернета вещей «Аура-360» для самовосстановления	202
5.3.3. Доработка операционной системы FenixOS на основе микроядра	204
5.3.4. «Паспортизация» стека протокола TCP/IP в размерностях	206
5.3.5. Алгоритм контроля семантики стека протоколов TCP/IP.....	207
5.4. Пример разработки самовосстанавливающейся системы хранения данных.....	211
5.4.1. Ограничения известных систем хранения данных	211
5.4.2. Выбор SDS-решений для самовосстановления	213
5.4.3. Решение на основе ОС Windows Server 2016 (2013)	215
5.4.4. Решения на основе ОС RAIDIX.....	216
5.4.5. Решения на основе FC- и NAS-кластеров	217
Заключение	223
Литература.....	225