

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
«ЮЖНЫЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Инженерно-технологическая академия

Ю. А. БРЮХОМИЦКИЙ

ИСКУССТВЕННЫЕ ИММУННЫЕ СИСТЕМЫ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Учебное пособие

Ростов-на-Дону – Таганрог
Издательство Южного федерального университета

2019

УДК 004.932(075.8) + 004.85(075.8)

ББК 32.973-018.2

Б898

*Печатается по решению кафедры информационной безопасности
Института компьютерных технологий и информационной
безопасности Южного федерального университета
(протокол № 6 от 6 марта 2019 г.)*

Рецензенты:

заведующий кафедрой информационной безопасности телекоммуникационных систем Института компьютерных технологий и информационной безопасности ЮФУ, доктор технических наук, профессор *К. Е. Румянцев*
директор ООО «Инженерный центр «Интегра», г. Таганрог, кандидат технических наук *А. С. Басан*

Брюхомицкий, Ю. А.

Б898 Искусственные иммунные системы в информационной безопасности : учебное пособие / Ю. А. Брюхомицкий ; Южный федеральный университет. – Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2019. – 147 с.

ISBN 978-5-9275-3212-4

Пособие содержит описание подходов, методов и средств аппарата искусственных иммунных систем в информационной безопасности.

Ориентировано на специалистов, аспирантов и студентов, работающих и обучающихся по направлениям и специальностям в области информационной безопасности.

УДК 004.932(075.8) + 004.85(075.8)

ББК 32.973-018.2

ISBN 978-5-9275-3212-4

© Южный федеральный университет, 2019

© Брюхомицкий Ю. А., 2019

© Оформление. Макет. Издательство

Южного федерального университета, 2019

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	3
1. ЕСТЕСТВЕННАЯ ИММУННАЯ СИСТЕМА	6
1.1. Принципы функционирования иммунной системы	6
1.2. Информационно-вычислительные аспекты иммунной систем	10
1.3. Сопоставление нервной и иммунной систем и их моделей	12
2. МОДЕЛИРОВАНИЕ ИММУННОЙ СИСТЕМЫ	15
2.1. Общие принципы моделирования иммунной системы	15
2.2. Модель иммунной сети	16
2.3. Модели отрицательного отбора	17
2.3.1. Модель отрицательного отбора со строковым представлением данных	18
2.3.2. Модель отрицательного отбора с двойной пластичностью	21
2.3.3. Модель отрицательного отбора с числовым представлением данных	31
2.4. Модель клональной селекции	35
2.5. Модель гиперклетки	37
3. ИСКУССТВЕННЫЕ ИММУННЫЕ СИСТЕМЫ В КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ	41
3.1. Аналогии в обеспечении компьютерной и иммунологической безопасности	41
3.2. Иммунологический мониторинг информационных процессов в компьютерных системах	44
3.2.1. Иммунологический мониторинг информационных процессов на основе классической модели отрицательного отбора	45
3.2.2. Иммунологический мониторинг информационных процессов на основе ускоренной модели отрицательного отбора	49
3.2.3. Иммунологический мониторинг информационных процессов на основе модели отрицательного отбора с полным перебором	54
3.2.4. Правила принятия решений по итогам иммунологического мониторинга	58
3.3. Обнаружение аномалий информационных процессов	59
3.3.1. Иммунологический способ обнаружения аномалий на основе анализа последовательностей системных вызовов	60

3.3.2. Иммунологический способ обнаружения аномалий на основе анализа сетевого трафика	66
3.4. Обнаружение вирусов	70
3.4.1. Искусственная иммунная система для обнаружения вирусов	71
3.5. Иммунологические технологии идентификации личности по динамическим биометрическим параметрам	81
3.5.1. Иммунологический клавиатурный мониторинг пользователей компьютерных систем	83
3.5.1.1. Клавиатурный мониторинг на основе иммунологической модели отрицательного отбора со строковым представлением данных	85
3.5.1.2. Клавиатурный мониторинг на основе цепочного метода и иммунологической модели отрицательного отбора со строковым представлением данных	93
3.5.1.3. Клавиатурный мониторинг на основе цепочного метода и иммунологической модели отрицательного отбора с числовым представлением данных	100
3.5.1.4. Клавиатурный мониторинг на основе цепочного метода и иммунологической модели клональной селекции с числовым представлением данных	103
3.5.2. Иммунологическая верификация личности по рукописи	106
3.5.2.1. Иммунологическая верификация личности по рукописи на основе модели отрицательного отбора со строковым представлением данных	108
3.5.2.2. Иммунологическая верификация личности по рукописи на основе модели отрицательного отбора с числовым представлением данных	116
3.5.2.3. Иммунологическая верификация личности по рукописи на основе модели клональной селекции с числовым представлением данных	119
3.5.3. Иммунологическая верификация личности по голосу	126
3.5.4. Технологии идентификации личности по динамическим биометрическим параметрам при совмещенном использовании ИИС и ИНС	134
ЗАКЛЮЧЕНИЕ	138
СПИСОК ЛИТЕРАТУРЫ	139