

ОГЛАВЛЕНИЕ

Введение	3
Глава 1. ОСНОВЫ АНАЛИЗА ЭПИДЕМИЧЕСКИХ ПРОЦЕССОВ, ПРОТЕКАЮЩИХ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ.	7
1.1. Актуальность противодействия атакам вредоносного программного обеспечения	7
1.2. Информационно-телекоммуникационная сеть как объект внедрения вредоносного программного обеспечения	11
1.3. Многообразие вредоносного программного обеспечения вирусного характера	14
1.4. Многообразие антивирусного программного обеспечения	31
1.5. Особенности моделирования вирусных эпидемий	37
Глава 2. ВИРУСНЫЕ ЭПИДЕМИИ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ: ОЦЕНКА ВЕРОЯТНОСТИ ЗАРАЖЕНИЯ ЭЛЕМЕНТА СЕТИ.	43
2.1. Входящий поток	43
2.2. Заражение элемента сети различными видами вирусов	45
2.3. Оценка вероятностей реализации различных этапов вирусной атаки.	59
2.3.1. Вероятностная оценка процесса инфекционного заражения элемента сети.	59
2.3.2. Вероятностная оценка процесса излечения зараженного элемента сети.	60
2.3.3. Вероятностная оценка процесса латентного инфицирования элемента сети	63
2.3.4. Вероятностная оценка процесса выхода из строя зараженного элемента сети.	65

Глава 3. РИСК-МОДЕЛИ ЭПИДЕМИЧЕСКИХ ПРОЦЕССОВ В ОДНОРОДНЫХ СЕТЯХ	69
3.1. Математические модели процесса развития информационных алгоритмов на примере SIR-модели	69
3.2. Риск-оценки процесса распространения информационной инфекции для SI-модели	73
3.2.1. Методика построения дискретной SI-модели	73
3.2.2. Риск-анализ и оценка эпистойкости сети в условиях распространения эпидемии по модели SI	76
3.3. Риск-анализ процесса распространения информационной инфекции по модели SIS	78
3.3.1. Методика построения дискретной SIS-модели	78
3.3.2. Риск-анализ и оценка эпистойкости сети в условиях распространения информационной эпидемии по модели SIS	80
3.4. Оценка рисков процесса распространения и риск-оценки информационной инфекции для SEIS-модели	82
3.4.1. Методика построения дискретной SEIS-модели	82
3.4.2. Риск-анализ и оценка эпистойкости сети в условиях распространения информационной эпидемии по модели SEIS	86
3.5. Риск-анализ процесса распространения информационной инфекции по модели SIR	88
3.5.1. Методика построения дискретной SIR-модели	88
3.5.2. Риск-анализ и оценка эпистойкости сети в условиях распространения информационной инфекции по модели SIR	92
3.6. Оценка рисков процесса распространения инфекции для SEIR-модели	94
3.6.1. Методика построения дискретной SEIR-модели	94
3.6.2. Риск-анализ и оценка эпистойкости сети в условиях распространения информационной эпидемии по модели SEIR	98
Глава 4. ДИСКРЕТНЫЕ РИСК-МОДЕЛИ РАЗВИТИЯ ЭПИДЕМИЙ В ГЕТЕРОГЕННЫХ СЕТЯХ	101
4.1. Обзор моделей эпидемий в гетерогенных сетях	101
4.1.1. Разновидности эпидемических моделей и сетей	101
4.1.2. Топологическое многообразие сетей в контексте их эпистойкости	104

4.1.3. Особенности аналоговых моделей вирусно-инфицированных сетей.	108
4.1.4. Аналоговые эпидемические модели, учитывающие корреляцию.	115
4.2. Многослойная формализация гетерогенных сетей.	123
4.2.1. Сущность дискретных моделей послойной формализации.	123
4.2.2. Дискретные модели многослойного риск-анализа.	129
4.2.3. Микрофрактал дискретной модели заражения.	136
Глава 5. СЕТЕВЫЕ ЧЕРВИ: МОДЕЛИ ИНФИЦИРОВАНИЯ СЕТЕЙ	141
5.1. Анализ особенностей и разновидностей сетевых червей.	141
5.1.1. Особенности сетевых червей как класса вредоносных программ.	141
5.1.2. Классификация вредоносного программного обеспечения вирусного характера типа сетевых червей.	143
5.2. Дискретные модели инфицирования для различных разновидностей сетевых червей.	149
5.2.1. Простейшая модель инфицирования.	149
5.2.2. Модель инфицирования с учетом мутации.	150
5.2.3. Модель инфицирования с учетом латентности.	152
5.2.4. Модель инфицирования по образу файлового вируса.	154
Глава 6. КОМПЬЮТЕРНЫЕ ЧЕРВИ КАК ИНСТРУМЕНТ ДЕСТРУКТИВНОГО ВОЗДЕЙСТВИЯ НА ПОЧТОВЫЕ СЕТИ	156
6.1. Статистика ущербов и частот атак почтовыми червями на структуры сетевого характера.	158
6.2. Классификация почтовых червей.	162
6.3. Защита сети от атак почтовым червем.	163
6.4. Эпидемический процесс, порождаемый в сетях почтовыми червями.	175
6.4.1. Проникновение почтовых червей в сеть.	175
6.4.2. Этап активации почтовых червей.	176
6.4.3. Этап распространения почтовых червей.	177
6.4.4. Реализация почтовым червем деструктивных воздействий.	180
6.5. Исследование сети электронной почты.	181

6.6. Дискретные модели инфицирования для различных разновидностей почтовых червей.	187
6.6.1. Модель без реинфекции с мутацией почтового червя	189
6.6.2. Модель без реинфекции и без мутации	191
6.6.3. Модель с реинфекцией и мутацией	193
6.6.4. Модель без мутации и реинфицирования	195
6.6.5. Модель с мутацией и без реинфицирования.	198
Глава 7. IM-, IRC- и P2P-ЧЕРВИ: МОДЕЛИ ИНФИЦИРОВАНИЯ ГЕТЕРОГЕННЫХ СЕТЕЙ	201
7.1. IM-черви как инструмент деструктивного воздействия на гетерогенные сети	201
7.1.1. Особенности IM-червей	201
7.1.2. Модели инфицирования IM-червями без мутации	202
7.1.3. Модель инфицирования IM-червями с мутацией	208
7.2. IRC-черви как инструмент деструктивного воздействия на гетерогенные сети	211
7.2.1. Специфика заражения IRC-червем	211
7.2.2. Модель инфицирования IRC-червем с учетом мутации	217
7.3. P2P-черви как инструмент деструктивного воздействия на гетерогенные сети	219
7.3.1. Описание и классификация P2P-червей	219
7.3.2. Модель инфицирования P2P-червей без учета его мутации.	221
7.3.3. Модель инфицирования P2P-червем с мутацией.	226
Заключение	229
Библиографический список	231
Приложение. ПРОГРАММНЫЙ КОМПЛЕКС «NETEPIDEMIC»	246
1. Структура данных	246
2. Технологическое обеспечение.	249
3. Лингвистическое обеспечение	258
4. Пример применения программного комплекса «Netepidemic» для моделирования процессов диффузии контента в социальной сети Facebook	258