

НАУЧНАЯ МЫСЛЬ

Бизнес-
информатика

*В.И. Новосельцев, С.С. Кочедыков,
Д.Е. Орлова, К.А. Плющик*

**КОНФЛИКТНО-АКТИВНОЕ УПРАВЛЕНИЕ
ПРОЕКТАМИ РАЗВИТИЯ
СИСТЕМ ОБЕСПЕЧЕНИЯ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ИНФОКОММУНИКАЦИОННЫХ СЕТЕЙ**



НАУЧНАЯ МЫСЛЬ

СЕРИЯ ОСНОВАНА В 2008 ГОДУ

**В.И. НОВОСЕЛЬЦЕВ
С.С. КОЧЕДЫКОВ
Д.Е. ОРЛОВА
К.А. ПЛЮЩИК**

**КОНФЛИКТНО-АКТИВНОЕ УПРАВЛЕНИЕ
ПРОЕКТАМИ РАЗВИТИЯ
СИСТЕМ ОБЕСПЕЧЕНИЯ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ИНФОКОММУНИКАЦИОННЫХ СЕТЕЙ**

МОНОГРАФИЯ

Под редакцией *В.И. Новосельцева*

Электронно-
Библиотечная
знаниум.com

Москва
ИНФРА-М
2023

УДК 004.056+005.8(075.4)
ББК 16.8:65стд1-21
Н65

Авторы:

Новосельцев В.И., доктор технических наук, старший научный сотрудник, профессор Воронежского института ФСИИ России;

Кочедыков С.С., кандидат технических наук, доцент, начальник кафедры Воронежского института ФСИИ России;

Орлова Д.Е., кандидат технических наук, преподаватель Воронежского института ФСИИ России;

Плющик К.А., адъюнкт Воронежского института ФСИИ России

Рецензенты:

Россихина Л.В., доктор технических наук, доцент, профессор Воронежского института ФСИИ России;

Гончаров И.В., кандидат технических наук, доцент, генеральный директор АО «Научно-производственное объединение «Инфобезопасность»»

Новосельцев В.И.

Н65 Конфликтно-активное управление проектами развития систем обеспечения информационной безопасности инфокоммуникационных сетей : монография / В.И. Новосельцев, С.С. Кочедыков, Д.Е. Орлова, К.А. Плющик; под ред. В.И. Новосельцева. — Москва: ИНФРА-М, 2023. — 235 с. — (Научная мысль). — DOI 10.12737/1921360.

ISBN 978-5-16-018194-3 (print)

ISBN 978-5-16-111199-4 (online)

Объектом изучения в монографии выступает конфликт «система обеспечения информационной безопасности инфокоммуникационных сетей критически важных объектов социально-экономической инфраструктуры — злоумышленник (преступный элемент)». Предметом исследования являются вопросы разработки методологии конфликтно-активного управления проектами развития систем обеспечения информационной безопасности этих сетей, включая модели поддержки принятия проектных решений. Теоретическую базу изложенного составляют положения системного анализа, теории управления и принятия решений, теории активных систем, теории информационной безопасности, теории математического моделирования и конфликта.

Предназначена для научных работников и специалистов, занимающихся проблемами обеспечения информационной безопасности инфокоммуникационных объектов социально-экономического профиля. Будет полезна аспирантам и студентам старших курсов, обучающимся по научной специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность».

УДК 004.056+005.8(075.4)

ББК 16.8:65стд1-21

ISBN 978-5-16-018194-3 (print)
ISBN 978-5-16-111199-4 (online)

© Новосельцев В.И., Кочедыков С.С.,
Орлова Д.Е., Плющик К.А., 2023

ОГЛАВЛЕНИЕ

Введение	7
Глава 1. КРАТКАЯ ХАРАКТЕРИСТИКА ПРОТИВОБОРСТВУЮЩИХ СТОРОН В КОНФЛИКТЕ «СИСТЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОКОММУНИКАЦИОННЫХ СЕТЕЙ – ЗЛОУМЫШЛЕННИК (ПРЕСТУПНЫЙ ЭЛЕМЕНТ)»	13
1.1. Основные направления деструктивных воздействий на инфокоммуникационные сети критически важных объектов социально-экономической инфраструктуры	13
1.2. Особенности построения систем обеспечения информационной безопасности инфокоммуникационных сетей критически важных объектов социально-экономической инфраструктуры	23
Глава 2. ОСНОВНЫЕ ПОЛОЖЕНИЯ МЕТОДОЛОГИИ КОНФЛИКТНО-АКТИВНОГО УПРАВЛЕНИЯ ПРОЕКТАМИ РАЗВИТИЯ СИСТЕМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОКОММУНИКАЦИОННЫХ СЕТЕЙ	35
2.1. Концепция и общая схема конфликтно-активного управления проектами развития систем обеспечения информационной безопасности инфокоммуникационных сетей	35
2.2. Виды неопределенностей при управлении проектами развития систем обеспечения информационной безопасности инфокоммуникационных сетей и способы их устранения	41
2.3. Структурная модель конфликтно-активного управления проектами развития систем обеспечения информационной безопасности инфокоммуникационных сетей	43
2.4. Показатели качества решений по управлению проектами развития систем обеспечения информационной безопасности инфокоммуникационных сетей	54
Глава 3. ОЦЕНКА СВОЕВРЕМЕННОСТИ ПРЕДОСТАВЛЕНИЯ ИНФОРМАЦИИ ИНФОКОММУНИКАЦИОННОЙ СЕТЬЮ В УСЛОВИЯХ ДЕСТРУКТИВНЫХ ВОЗДЕЙСТВИЙ	68
3.1. Постановка задачи и метод решения	68
3.2. Оценка своевременности на структурном уровне представления инфокоммуникационной сети	71

3.3. Оценка своевременности на информационном уровне представления инфокоммуникационной сети	74
3.4. Алгоритм оценки своевременности	78
Глава 4. ОЦЕНКА ФУНКЦИОНАЛЬНОЙ РАБОТОСПОСОБНОСТИ ИНФОКОММУНИКАЦИОННОЙ СЕТИ В УСЛОВИЯХ ДЕСТРУКТИВНЫХ ВОЗДЕЙСТВИЙ	80
4.1. Постановка задачи	80
4.2. Алгоритм оценки функциональной работоспособности инфокоммуникационной сети в условиях деструктивных воздействий	82
4.3. Оценка риска нарушения функциональной работоспособности инфокоммуникационной сети, подвергшейся деструктивным воздействиям	89
Глава 5. ОЦЕНКА ЦЕЛОСТНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ИНФОКОММУНИКАЦИОННОЙ СЕТИ В УСЛОВИЯХ ДЕСТРУКТИВНЫХ ВОЗДЕЙСТВИЙ	94
5.1. Постановка задачи	94
5.2. Формализация структуры программного обеспечения инфокоммуникационных сетей	97
5.3. Алгоритм оценки целостности программного обеспечения инфокоммуникационных сетей	100
Глава 6. ОЦЕНКА БЫСТРОДЕЙСТВИЯ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	105
6.1. Формулировка задачи	105
6.2. Сущность подхода и описание модели	106
6.3. Алгоритм оценки быстродействия системы обеспечения информационной безопасности	111
Глава 7. КООРДИНАЦИЯ РЕШЕНИЙ ПРИ УПРАВЛЕНИИ ПРОЕКТАМИ РАЗВИТИЯ СИСТЕМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОКОММУНИКАЦИОННЫХ СЕТЕЙ	112
7.1. Основные теоретические положения и формализация задачи	112
7.2. Алгоритмы оптимизации координирующих решений	119

Глава 8. КЛАСТЕР-ИДЕНТИФИКАЦИИ СИТУАЦИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	124
8.1. Кластер-идентификация ситуаций информационной безопасности по детерминированным признакам	125
8.2. Кластер-идентификация ситуаций информационной безопасности по вероятностным признакам	134
8.3. Кластер-идентификация ситуаций информационной безопасности по понятийным признакам	139
8.4. Обобщенный алгоритм кластер-идентификации ситуаций информационной безопасности	147
8.5. Идентификации типов деструктивных воздействий с использованием придаваемых средств защиты информации	148
8.6. Идентификации типов деструктивных воздействий с использованием встраиваемых средств защиты информации	152
Глава 9. МОДЕЛИРОВАНИЕ КОНФЛИКТА «СИСТЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ – ЗЛОУМЫШЛЕННИК (ПРЕСТУПНЫЙ ЭЛЕМЕНТ)»	156
9.1. Исходные положения	156
9.2. Формализация конфликта	157
9.3. Алгоритм моделирования	161
Глава 10. МОДЕЛЬ ОПТИМИЗАЦИИ ПЛАН-ГРАФИКА ВНЕДРЕНИЯ ПРОЕКТА РАЗВИТИЯ СИСТЕМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОБЪЕКТАХ ИНФОКОММУНИКАЦИОННОЙ СЕТИ	165
10.1. Формулировка задачи и метод решения	165
10.2. Формализация и математическая модель	167
10.3. Алгоритм оптимизации	169
Глава 11. СТИМУЛИРОВАНИЕ ИСПОЛНИТЕЛЕЙ ПРОЕКТОВ РАЗВИТИЯ СИСТЕМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОКОММУНИКАЦИОННЫХ СЕТЕЙ	174
11.1. Критерии и механизмы стимулирования	175
11.2. Определение размера премиального фонда и его распределение между исполнителями проекта	178
11.3. Стимулирование путем урегулирования конфликтных ситуаций «руководитель проекта – исполнители»	180

Глава 12. КОМПЬЮТЕРНЫЙ КОМПЛЕКС ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ПРИ УПРАВЛЕНИИ ПРОЕКТАМИ РАЗВИТИЯ СИСТЕМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОКОММУНИКАЦИОННЫХ СЕТЕЙ	186
12.1. Назначение и принципы построения комплекса	186
12.2. Состав и структура комплекса	187
12.3. Режимы работы комплекса	193
12.4. Основные технические характеристики комплекса	194
12.5. Результаты тестирования комплекса	198
Заключение	200
Список использованной литературы	203
Приложение 1. Системное понимание сущности конфликта и его свойств	213
Приложение 2. Краткая история развития и сущность рефлексивного подхода в управлении	229