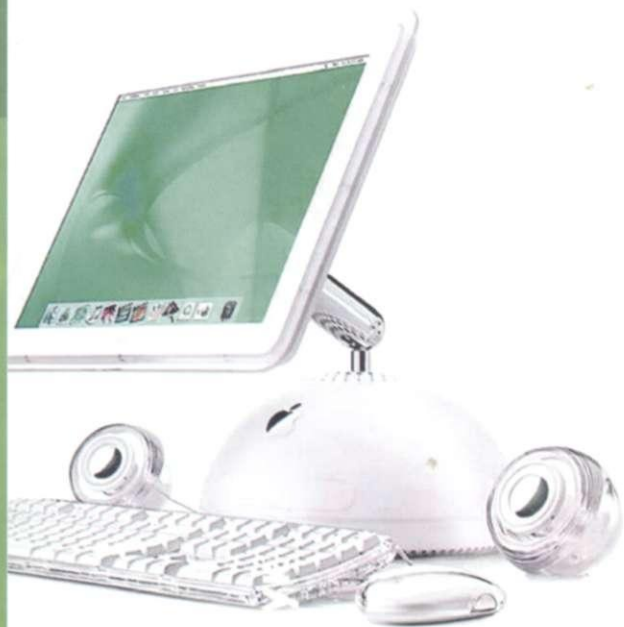


Р. В. Грищук

**ТЕОРЕТИЧНІ ОСНОВИ МОДЕЛЮВАННЯ
процесів нападу на інформацію
методами теорій диференціальних ігор
та диференціальних перетворень**

Монографія



МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЖИТОМИРСЬКИЙ ВІЙСЬКОВИЙ ІНСТИТУТ ІМЕНІ С. П. КОРОЛЬОВА
НАЦІОНАЛЬНОГО АВІАЦІЙНОГО УНІВЕРСИТЕТУ

Р. В. ГРИЩУК

**Теоретичні основи моделювання
процесів нападу на інформацію
методами теорій диференціальних ігор
та диференціальних перетворень**

М о н о г р а ф і я

Житомир
РУТА
2010

ББК 22.12
Г85
УДК 004.9: 517.978.2

Гришук Р. В.

Г85 Теоретичні основи моделювання процесів нападу на інформацію методами теорій диференціальних ігор та диференціальних перетворень: Монографія / Р. В. Гришук. - Житомир : Рута, 2010. - 280 с: іл.
ISBN 978-617-581-033-0

У монографії розглядаються теоретичні основи моделювання процесів нападу на інформацію методами теорій диференціальних ігор та диференціальних перетворень. Розроблено спектральні моделі процесів нападу на інформацію та запропоновано моделі їх векторної оптимізації. Подано основи моделювання процесів нападу на інформацію на графах. Надано рекомендації щодо застосування розроблених основ та наведено модельні приклади.

Для фахівців у галузі захисту інформації, наукових працівників та інженерно-технічних спеціалістів. Монографія може бути корисною для аспірантів, магістрантів і студентів, котрі спеціалізуються у сфері управління інформаційною безпекою та систем захисту інформації.

ББК 22.12
УДК 004.9: 517.978.2

*Рекомендовано вченою радою
Житомирського військового інституту імені С. П. Корольова
Національного авіаційного університету
до друку та використання в навчальному процесі
(протокол № 2 від 25 жовтня 2010 року)*

Рецензенти:

Баранов В. Л. — доктор технічних наук, професор,
заслужений діяч науки і техніки України.
Хорошко В. О. — доктор технічних наук, професор.

ISBN 978-617-581-033-0

© Р. В. Гришук, 2010
© ПП «РУТА», 2010



*Світлій пам'яті видатного вченого, винахідника,
доктора технічних наук, професора,
заслуженого діяча науки і техніки України
Баранова Володимира Леонідовича
присвячую ...*

Золота осінь 2005 року докорінно змінила мою долю. Я мав нагоду познайомитися з видатним вченим, винахідником доктором технічних наук, професором, заслуженим діячем науки і техніки України Барановим Володимиром Леонідовичем, який вже з перших хвилин спілкування знайшов спільну тему для цікавої та тривалої наукової дискусії.

Перше, що мене вразило - це щирий і відкритий погляд вченого, очі якого випромінювали доброту та справжню батьківську турботу. Володимир Леонідович був прекрасним педагогом та талановитим ученим. Будучи глибоко освіченою і скромною людиною, інтелектуалом та видатним математиком, саме він переконав мене в тому, що всі мої проблеми пов'язані з розв'язанням систем інтегральних рівнянь Фредгольма першого роду з невідомими параметрами в апаратних функціях, можуть бути подолані. Як показав час, це було справді так.

Професор Баранов В. Л. зробив суттєвий внесок у розвиток вітчизняної науки і техніки. Ним розвинено технологію системоаналогового та квазіаналогового моделювання, моделювання на графах. Завдяки його натхненній праці істотного розвитку набули теорії диференціальних ігор та диференціальних перетворень.

Високий професіоналізм, людяність, порядність, принциповість, цілковита відданість обраній справі, дотримання даного слова, любов до Батьківщини - ось далеко не всі чесноти видатного вченого.

Саме він, мій дорогий та вельмишановний вчитель професор Баранов В. Л., був, є і буде для мене взірцем найвищого патріотизму, відданості служіння людям та своїй державі. Життєве кредо Володимира Леонідовича — "Людям нужно помогать!" І він допомагав щиро, не жаліючи себе, працюючи на повну силу свого духу та розуму.

На момент кінцевого редагування монографії 26 вересня 2010 року наука зазнала тяжкої втрати: перестало битися серце цієї доброї та чуйної Людини.

Вважаю за свій обов'язок - глибоко шанувати пам'ять видатного вченого, а надалі бути гідним учнем його наукової школи, яка складається з 5 докторів та 25 кандидатів наук.

Ось які слова під час одного з робочих моментів написав мені Володимир Леонідович:

Руслану
Грицику
с пожеланиями
успехов в науке
12.04.2006

З повагою та глибокою вдячністю
учень професора Баранова Володимира Леонідовича
кандидат технічних наук Руслан Грищук

ЗМІСТ

ПЕРЕДМОВА	9
РОЗДІЛ 1. АНАЛІЗ СУЧАСНОГО СТАНУ ПРОБЛЕМИ МОДЕЛЮВАННЯ ПРОЦЕСІВ НАПАДУ НА ІНФОРМАЦІЮ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ ПРАКТИЧНИМИ ЗАВДАННЯМИ.	14
1.1. Аналіз стану проблеми.....	14
1.2. Дослідження та аналіз особливостей реалізації процесу нападу на інформацію за відомими моделями.....	16
1.2.1. Статичні моделі.....	20
1.2.2. Статистичні моделі.....	33
1.2.3. Динамічні моделі.....	38
1.3. Аналіз відомих підходів до вирішення проблеми захисту інформації на основі теорії ігор.....	41
1.4. Обґрунтування доцільності застосування теорій диференціальних ігор та диференціальних перетворень для моделювання процесів нападу на інформацію.....	47
1.4.1. Аналіз можливостей застосування теорії диференціальних ігор.....	47
1.4.2. Аналіз можливостей застосування теорії диференціальних перетворень. Основні поняття та визначення.....	53
РОЗДІЛ 2. ОДНОКРИТЕРІЙНІ ДИФЕРЕНЦІАЛЬНО-ІГРОВІ МОДЕЛІ ПРОЦЕСІВ НАПАДУ НА ІНФОРМАЦІЮ.	61
2.1. Концептуальні основи кількісного підходу.....	61
2.2. Диференціально-ігрова графова модель процесу нападу на інформацію.....	63
2.3. Метод диференціально-ігрового Р-моделювання процесів нападу на інформацію на основі однокритерійної моделі.	74

2.4.	Диференціально-ігрова спектральна модель процесу нападу на інформацію на основі диференціальних перетворень	80
2.5.	Диференціально-ігрова SIGW спектральна P-модель	93
2.6.	Диференціально-ігрова розгалужена спектральна P-модель	105
2.7.	Спектральна P-модель процесу нападу на інформацію при нестационарній природі потоків захисних дій та інформаційних атак	114

РОЗДІЛ 3. ТОЧНІ ДИФЕРЕНЦІАЛЬНО-ІГРОВІ НЕТЕЙЛОРІВСЬКІ ТА ГІБРИДНІ МОДЕЛІ ПРОЦЕСІВ НАПАДУ НА ІНФОРМАЦІЮ ... 123

3.1.	Диференціально-ігрова нетейлорівська модель	123
3.2.	Метод гібридного P-L-моделювання процесів нападу на інформацію	128
3.3.	Диференціально-ігрова GIGW гібридна P-L-модель	132
3.4.	Диференціально-ігрова гібридна P-L-модель процесу нападу на інформацію з урахуванням показника якісного функціонування системи захисту інформації	134
3.5.	Неперервна дискретна диференціально-ігрова модель	140

РОЗДІЛ 4. БАГАТОКРИТЕРІЙНІ ДИФЕРЕНЦІАЛЬНО-ІГРОВІ МОДЕЛІ ПРОЦЕСІВ НАПАДУ НА ІНФОРМАЦІЮ 146

4.1.	Загальний аналіз багатокритерійних моделей оптимізації векторного критерію	146
4.2.	Багатокритерійна диференціально-ігрова модель процесу нападу на інформацію на основі інтегральної оптимальності	149
4.3.	Багатокритерійна диференціально-ігрова модель процесу нападу на інформацію на основі нелінійної схеми компромісів	163

РОЗДІЛ 5. ВЕРИФІКАЦІЯ ТА ДОСЛІДЖЕННЯ ДИФЕРЕНЦІАЛЬНО-ІГРОВИХ МОДЕЛЕЙ 176

5.1.	Модельні приклади	176
5.1.1.	Дослідження диференціально-ігрової спектральної P-моделі на три інформаційні стани	176

5.1.2.	Дослідження диференціально-ігрової GIGW гібридної P-L-моделі.....	180
5.1.3.	Дослідження диференціально-ігрових моделей процесів нападу на інформацію при нестационарній природі потоків захисних дій та інформаційних атак .	182
5.1.4.	Дослідження багатокритерійної диференціально-ігрової моделі інтегральної оптимальності в задачах моделювання процесів нападу на інформацію P-перетвореннями.....	183
5.2.	Верифікація та дослідження диференціально-ігрових спектральних P- та гібридних P-L-моделей.....	184
5.3.	Застосування диференціально-ігрового методу для аналізу надійності систем захисту інформації на основі їх спектральних P-моделей.....	194
5.3.1.	Практичні рекомендації.....	207
5.4.	Застосування диференціально-ігрових моделей для розробки шаблонів поведінки Web-серверів.....	210
5.4.1.	Диференціально-ігровий шаблон нормальної поведінки Web-сервера.....	210
5.4.2.	Диференціально-ігровий шаблон атаки на Web-сервер.....	227
	ДОДАТОК А. Основні диференціальні спектри та дії над ними	245
	ДОДАТОК Б. Вихідні дані log-файлів для розробки шаблону нормальної поведінки Web-сервера Apache 2.2.10 (Linux SUSE).	251
	ПІСЛЯМОВА.....	253
	ЛІТЕРАТУРА.....	258

CONTENTS IN BRIEF

INTRODUCTION.....	9
CHAPTER 1. Analysis of Modern State Problems in Differential-Gaming Modeling of Information Attacking Process and its Connection With Significant Practical Tasks	14
CHAPTER 2. Singlecriteria Differential-Gaming Models of Information Attacking Process	61
CHAPTER 3. Precise Differential-Gaming Models of Information Attacking Process	123
CHAPTER 4. Multicriteria Differential-Gaming Models of Information Attacking Process	146
CHAPTER 5. Verification and Examining of Differential-Gaming Models.....	176
APPENDIX.....	245
INFERENCE.....	253
BIBLIOGRAPHY.....	258