

**ИНФОРМАЦИОННАЯ
БЕЗОПАСНОСТЬ
СИСТЕМ
ОРГАНИЗАЦИОННОГО
УПРАВЛЕНИЯ**

Теоретические
ОСНОВЫ

Том 1

НАУКА

РОССИЙСКАЯ АКАДЕМИЯ НАУК
ИНСТИТУТ ПРОБЛЕМ ПЕРЕДАЧИ ИНФОРМАЦИИ

Информационная безопасность СИСТЕМ организационного управления

Теоретические основы

В двух томах

Том 1

Под редакцией
академика Н.А. Кузнецова,
доктора технических наук В.В. Кульбы



МОСКВА НАУКА 2006



УДК 519.8
ББК 22.18
ИЗЗ

Коллектив авторов:

Н.А.Кузнецов — академик, *В.В.Кульба* — д.т.н., проф.,
Е.А.Микрин — д.т.н., проф., *С.С.Ковалевский* — д.т.н.,
Б.В.Павлов — д.т.н., *С.А.Косяченко* — д.т.н.,
Г.Г.Малинецкий — д.ф.-м.н, *Н.И.Архипова* — д.э.н., проф.,
А.В.Кульба — д.т.н., проф., *А.Е.Волков* — д.т.н.,
А.Б.Шелков — к.т.н., с.н.с., *С.А.Власов* — к.т.н., с.н.с.,
Д.А.Кононов — к.т.н., с.н.с., *А.Н.Шубин* — к.т.н., с.н.с.,
И.В.Чернов — к.т.н., с.н.с., *Ю.М.Гладков* — к.т.н., с.н.с.

Рецензенты:

академик *С.К.Коровин*,
доктор физико-математических наук *А.В. Лотов*

Информационная безопасность систем организационно-го управления. Теоретические основы : в 2 т. / Н.А. Кузнецов, В.В.Кульба, Е.А.Микрин и др. ; [отв. ред. Н.А.Кузнецов, В.В.Кульба] ; Ин-т проблем передачи информ. РАН. — М. : Наука, 2006. — ISBN 5-02-034145-2.

Т.1. — 2006. — 495 с. — ISBN 5-02-034146-0 (в пер.).

В монографии рассмотрены следующие вопросы: информационная безопасность в системах организационного управления на законодательном и организационном уровнях, информационная безопасность и информационное управление, методы защиты информации от несанкционированного доступа, обеспечение достоверности и сохранности информации. Цель книги — обзор, классификация и анализ уже имеющихся в этих областях теоретических разработок, ознакомление специалистов с новыми методами и способами защиты информации на ее различных уровнях, рекомендации в области обеспечения информационной безопасности.

Для научных работников и специалистов по информационной безопасности.

Темплан 2006-I-11

ISBN 5-02-034145-2

© Ин-т проблем передачи информации РАН,
2006

ISBN 5-02-034146-0 (т. 1)

© Редакционно-издательское оформление.
Издательство «Наука», 2006

СОДЕРЖАНИЕ

ТОМ 1

Введение	3
----------------	---

ЧАСТЬ I

Информационная безопасность в системах организационного управления на законодательном и организационном уровнях

1. Системы защиты информации на государственном уровне и их законодательная и нормативная база	13
1.1. Глобализация и информационное общество	13
1.2. Информационная безопасность государства. Государственная тайна	27
1.3. Законодательная и нормативная база информационной безопасности	51
1.4. Анализ влияния информационных технологий на социально-экономическое развитие общества в условиях глобализации	66
2. Информационные технологии в системах организационного управления	84
2.1. Понятие информации, ее свойства и характеристики	84
2.2. Особенности использования информации о состоянии внешней среды и управляемого объекта в организационных системах управления с обратной связью	93
2.3. Особенности создания информационного обеспечения систем организационного управления	100
2.4. Возможности использования современных информационных технологий в системах организационного управления	107
2.5. Информационное обеспечение управления в условиях чрезвычайных ситуаций	125

ЧАСТЬ II

Информационная безопасность и информационное управление

3. Основные положения информационного управления	135
3.1. Императив устойчивого развития	135
3.2. Методы управления и их характеристики	138
3.3. Информационное управление, характеристики и методы	141
3.4. Объекты информационного управления и их характеристики	163

3.5. Медиапланирование	172
3.6. Организационная структура подготовки и реализации информационного управления	188
3.7. Моделирование информационного управления с использованием знаковых графов	193
3.8. Средства информационного управления	197
3.9. Мониторинг в системах информационного управления	206
4. Теоретические основы информационного управления	212
4.1. Основные проблемы и задачи теоретического исследования информационного управления	212
4.2. Основные положения информационно-логического подхода	214
4.3. Основные положения системно-логического подхода	228
4.4. Основные положения структурно-социального подхода	235
4.5. Формализация стратегий информационного управления с использованием сценарного подхода	251
4.6. Моделирование и формирование сценариев информационного управления	299

ЧАСТЬ III

Методы защиты информации от несанкционированного доступа

5. Обеспечение информационной безопасности автоматизированных систем	315
5.1. Организационный уровень обеспечения информационной безопасности	315
5.2. Криптографические методы обеспечения информационной безопасности	329
5.3. Антивирусная защита автоматизированных систем	338
5.4. Удаленные атаки на автоматизированные системы	343
5.5. Межсетевое экранирование	348
5.6. Обеспечение физической защиты автоматизированных систем	355
5.7. Методы сокрытия информации на основе компьютерной стеганографии	368
6. Анализ и синтез систем защиты от несанкционированного доступа к данным	375
6.1. Механизмы и методы защиты	376
6.2. Модели и методы синтеза систем защиты информации	389
6.3. Использование сетей Петри с разноцветными маркерами для анализа эффективности и синтеза механизмов защиты данных в базах данных	392
6.4. Особенности отладки механизмов защиты	414
7. Мониторинг и аудит систем обеспечения информационной безопасности	455
7.1. Поддержание работоспособности автоматизированных систем	455
7.2. Использование систем регистрации информации для мониторинга информационной безопасности	459
7.3. Аудит систем обеспечения информационной безопасности	473
Список основных сокращений	480
Литература	484

ТОМ 2

Введение	3
----------------	---

ЧАСТЬ IV

Обеспечение достоверности и сохранности информации

8. Обеспечение достоверности при обработке данных в системах организационного управления	13
8.1. Методы обеспечения достоверности при обработке данных в системах организационного управления	13
8.2. Задачи анализа и синтеза систем контроля и обеспечение достоверности при обработке данных в СОУ	20
8.3. Методы контроля достоверности с использованием принципа обратной связи	29
8.4. Анализ предметных областей банков данных и построение оптимальных структур баз данных с учетом достоверности информации	72
8.5. Анализ систем обеспечения достоверности с использованием аппарата сетей Петри	125
9. Резервирование программных модулей и информационных массивов	156
9.1. Методы повышения сохранности программного и информационного обеспечения в СОУ	156
9.2. Стратегии резервирования и анализ их эффективности	161
9.3. Обобщенная модель резервирования программных модулей и информационных массивов	194
9.4. Резервирование информационных массивов в системах реального времени	208
10. Восстановление информации в СОУ	216
10.1. Характеристики и области эффективного применения методов восстановительного резервирования	216
10.2. Использование системной журнализации для восстановления информации в СОУ	229
10.3. Характеристики методов восстановления информационных массивов	231
11. Резервирование программных модулей и информационных массивов в сетях ЭВМ	250
11.1. Особенности использования информационной избыточности в сетях ЭВМ	250
11.2. Оперативное резервирование информационных массивов в сетях ЭВМ	259
11.3. Анализ эффективности методов восстановительного резервирования данных в сетях ЭВМ	283
11.4. Задачи оптимального резервирования массивов в сетях ЭВМ	297
11.5. Оптимизация оперативного резервирования данных в сетях ЭВМ	307
11.6. Оптимизация восстановительного резервирования данных в сетях ЭВМ	320
11.7. Методы уменьшения размерности задач оптимального резервирования данных в сетях ЭВМ	326

11.8. Определение состава и характеристик структурно-технологического резерва	333
11.9. Структурно-технологическое резервирование в сетях ЭВМ и его характеристики	338
12. Организация и планирование отладки и опытной эксплуатации систем обработки данных в СОУ	351
12.1. Особенности отладки программ в системах обработки данных	351
12.2. Методология планирования и организации системной отладки комплексов программ в СОУ	372
12.3. Задачи выбора оптимальной стратегии системной отладки комплексов программ	382
12.4. Методы решения задач выбора оптимальной стратегии системной отладки комплексов программ	391
12.5. Планирование отладочных работ на стадии рабочего проектирования	398
12.6. Методы оценки трудоемкости отладки и внесения изменений в модульное программное обеспечение	412
Список основных сокращений	422
Литература	426