

А. А. Малюк

ТЕОРИЯ ЗАЩИТЫ ИНФОРМАЦИИ



Горячая линия-Телеком



А. А. Малюк

**ТЕОРИЯ
ЗАЩИТЫ
ИНФОРМАЦИИ**

Москва
Горячая линия - Телеком
2014

УДК 004.056
ББК 32.973-018.2
М21

Рецензенты: доктор физ.-мат. наук, профессор *Г. О. Крылов*,
доктор техн. наук, профессор *М. П. Сычев*, доктор техн. наук,
профессор *А. А. Тарасов*.

Малюк А. А.

М21 Теория защиты информации. – М.: Горячая линия–Телеком,
2014. – 184 с., ил.
ISBN 978-5-9912-0246-6.

В книге предпринята попытка ответить на объективные потребности формирования концептуальных и методологических основ обеспечения информационной безопасности в процессе развития информационного общества. В ней изложены основы теории защиты информации, объединяющие широкий спектр проблем, связанных с обеспечением информационной безопасности в процессе генерирования, обработки, хранения и передачи информации в автоматизированных системах и на объектах информатизации. Анализируются различные подходы к моделированию систем и процессов защиты информации в условиях неполноты и недостоверности исходных данных. Особое внимание уделено эвристической составляющей процесса поиска наиболее рациональных решений в различных ситуациях защиты информации.

Для специалистов в области обеспечения информационной безопасности, будет полезна студентам и аспирантам высших учебных заведений, слушателям курсов повышения квалификации.

ББК 32.973-018.2

Адрес издательства в Интернет WWW.TECHBOOK.RU

Научное издание

Малюк Анатолий Александрович

ТЕОРИЯ ЗАЩИТЫ ИНФОРМАЦИИ

Редактор Ю. Н. Чернышов

Компьютерная верстка Ю. Н. Чернышова

Обложка художника В. Г. Ситникова

Подписано в печать 25.12.13. Формат 60×90 16. Усл. печ. л. 11,5. Тираж 500 экз. (2 завод - 250 экз.)

ISBN 978-5-9912-0246-6

© А. А. Малюк, 2012, 2014

© Издательство Горячая линия–Телеком, 2014

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ	3
Глава 1. СОВРЕМЕННЫЕ ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ	11
1.1. Проблемы защиты информации в общей совокупности информационных проблем современного общества ..	11
1.2. Ретроспективный анализ развития подходов к защите информации	18
1.3. Современная постановка задачи защиты информации	25
1.4. Перехода к интенсивным способам защиты информации	32
Глава 2. НАУЧНО-МЕТОДОЛОГИЧЕСКИЕ ОСНОВЫ ИНТЕНСИФИКАЦИИ ПРОЦЕССОВ ЗАЩИТЫ ИНФОРМАЦИИ	40
2.1. Определение и принципы формирования теории защиты информации	40
2.2. Методологический базис теории защиты информации	46
2.3. Развитие неформальных методов анализа процессов защиты информации	55
2.4. Моделирование процессов защиты информации	60
2.5. Основное содержание теории защиты информации ..	70
Глава 3. МЕТОДОЛОГИЯ ОЦЕНКИ УЯЗВИМОСТИ ИНФОРМАЦИИ	81
3.1. Понятие угрозы безопасности информации, системная классификация угроз	81
3.2. Показатели уязвимости информации	87
3.3. Методология оценки достоверности информационной базы прогнозирования показателей уязвимости информации	92
3.4. Модели оценки ущерба от реализации угроз безопасности информации	97
Глава 4. МЕТОДОЛОГИЯ ОПРЕДЕЛЕНИЯ ТРЕБОВАНИЙ К ЗАЩИТЕ ИНФОРМАЦИИ	104
4.1. Постановка задачи и методика определения требований к защите информации	104

4.2. Параметры защищаемой информации	107
4.3. Оценка факторов, влияющих на требуемый уровень защиты	115
4.4. Определение весов и классификация вариантов потенциально возможных условий защиты информации ..	119
Глава 5. МЕТОДОЛОГИЯ ФОРМИРОВАНИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ	128
5.1. Определение, типизация и стандартизация систем защиты информации.....	128
5.2. Адаптация и управление развитием систем защиты информации	133
5.3. Управление процессами функционирования систем защиты информации.....	141
Глава 6. ПЕРСПЕКТИВЫ РАЗВИТИЯ ТЕОРИИ И ПРАКТИКИ ЗАЩИТЫ ИНФОРМАЦИИ	152
6.1. Анализ гносеологии и прогноз развития теории защиты информации.....	152
6.2. Концепция специализированных центров защиты информации	159
6.3. Концепция развития межведомственной системы подготовки и переподготовки кадров в области обеспечения информационной безопасности.....	173
ЛИТЕРАТУРА	180