

Оглавление

Список основных сокращений	3
Предисловие	5
ЛЕКЦИЯ I	8
Введение	8
Наиболее острые проблемы сегодняшнего дня	13
Исторический очерк	14
Содержание курса	16

РАЗДЕЛ 1

СОВРЕМЕННЫЕ ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

ЛЕКЦИЯ II	19
Определение понятия «Информационная безопасность»	19
Общая схема обеспечения информационной безопасности	22
Проблема защиты информации	24
Анализ развития подходов к защите информации	27
Эмпирический, концептуально-эмпирический и теоретико-концептуальный подходы	31
ЛЕКЦИЯ III	39
Современная постановка задачи защиты информации	39
Основные факторы современного этапа	39
Основные концептуальные положения	41
Переход к интенсивным способам защиты информации	46
Кортеж концептуальных решений	48
Формирование баз исходных данных	49
Итоги раздела 1	53
Выводы по материалам раздела 1	53
Вопросы для повторения	54

РАЗДЕЛ 2**НАУЧНО-МЕТОДОЛОГИЧЕСКИЕ ОСНОВЫ
ИНТЕНСИФИКАЦИИ ПРОЦЕССОВ
ЗАЩИТЫ ИНФОРМАЦИИ**

ЛЕКЦИЯ IV	57
Определение и принципы формирования теории защиты информации	57
Общетеоретические принципы формирования теории	60
Теоретико-прикладные принципы	63
Методологический базис теории защиты информации	65
Методы теории нечетких множеств	65
Методы теории лингвистических переменных	66
Неформальные методы оценивания	67
Неформальные методы поиска оптимальных решений	70
ЛЕКЦИЯ V	75
Развитие неформальных методов анализа процессов защиты информации. Автоформализация знаний эксперта	75
Структура процесса принятия решений	77
Формирование базы данных	79
Формирование базы моделей	80
Принципы построения модели защиты от несанкционированного доступа	81
Монитор обращений	82
Правила разграничения доступа	83
Вербальная модель разграничения доступа	84
Модель Хартсона	85
Модель Лэмпсона, Грэхема, Деннинга	86
Модель Белла и Ла Падула	89
ЛЕКЦИЯ VI	91
Обобщенная модель процессов защиты информации	91
Энтропийный подход к моделированию	94
Модель системы обеспечения безопасности информации	97
ЛЕКЦИЯ VII	101
Основное содержание теории защиты информации	101
Стратегии защиты информации	102

Унифицированная технология автоматизированной обработки информации	105
Унифицированная концепция защиты информации	107
Итоги раздела 2	111
Выводы по материалам раздела 2	111
Вопросы для повторения	113

РАЗДЕЛ 3

МЕТОДОЛОГИЯ ОЦЕНКИ УЯЗВИМОСТИ ИНФОРМАЦИИ

ЛЕКЦИЯ VIII	117
Понятие угрозы безопасности информации	117
Подходы к классификации угроз	117
Системная классификация угроз	122
Показатели уязвимости информации	125
Базовый, обобщенный, общий и экстремальные показатели уязвимости	127
Учет интервала времени оценки	128
ЛЕКЦИЯ IX	130
Оценка достоверности информационной базы прогнозирования показателей уязвимости информации	130
Модификация фрагментов интегрированной базы данных	132
Методы обработки свидетельств	134
Применение методов фильтрации	136
Алгоритм оптимального фильтра Калмана	141
ЛЕКЦИЯ X	144
Понятие информационного риска	144
Модели оценки вероятности проявления угроз безопасности	146
Модели оценки ущерба от реализации угроз безопасности информации	147
Динамическая модель оценки потенциальных угроз	148
Модель оценки ущерба в терминах теории игр	150
Выводы по рассмотренным моделям	151
Итоги раздела 3	153
Выводы по материалам раздела 3	153
Вопросы для повторения	154

РАЗДЕЛ 4**МЕТОДОЛОГИЯ ОПРЕДЕЛЕНИЯ
ТРЕБОВАНИЙ К ЗАЩИТЕ ИНФОРМАЦИИ**

ЛЕКЦИЯ XI	157
Постановка задачи определения требований к защите информации	157
Методики определения требований к защите	158
Основные действующие документы Российской Федерации	159
Анализ применяемых методик	160
Подходы к преодолению недостатков действующих методик	162
Определение параметров защищаемой информации	162
Важность информации	163
Полнота информации	166
Адекватность информации	167
Релевантность информации	169
Толерантность информации	171
Оценка информации как объекта труда	171
ЛЕКЦИЯ XII	172
Оценка факторов, влияющих на требуемый уровень защиты	172
Формирование множества факторов	173
Определение весов и классификация вариантов потенциально возможных условий защиты информации	178
Использование методов кластерного анализа	181
Эмпирический подход к делению на классы	184
Итоги раздела 4	190
Выводы по материалам раздела 4	190
Вопросы для повторения	192

РАЗДЕЛ 5**МЕТОДОЛОГИЯ ФОРМИРОВАНИЯ
СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ**

ЛЕКЦИЯ XIII	195
Определение системы защиты информации	195
Типизация и стандартизация систем защиты информации	197
Высший уровень типизации и стандартизации	197

Средний уровень типизации и стандартизации	201
Низший уровень типизации и стандартизации	201
Адаптация и управление развитием систем защиты информации	202
Многокритериальный развивающийся объект.	202
Монотонный критерий	203
Формализация политики безопасности	205
Оценка эффективности процессов защиты.	207
ЛЕКЦИЯ XIV	212
Общая модель управления системой защиты	212
Основные макропроцессы управления	214
Методологические основы выработки управленческих решений	215
Особенности многокритериальных задач управления.	221
Контроль защищенности информации	223
ЛЕКЦИЯ XV	228
Комплексная политика защиты информации	228
Функции защиты	229
Задачи защиты	233
Средства и методы защиты.	239
Система защиты информации	240
Итоги раздела 5	241
Выводы по материалам раздела 5	241
Вопросы для повторения	243

РАЗДЕЛ 6

ПЕРСПЕКТИВЫ РАЗВИТИЯ ТЕОРИИ И ПРАКТИКИ ЗАЩИТЫ ИНФОРМАЦИИ

ЛЕКЦИЯ XVI	247
Анализ гносеологии развития теории защиты информации	247
Совершенствование теоретических основ защиты информации	249
Перевод защиты информации на индустриальную основу.	250
Расширение постановки задачи защиты.	
Обеспечение информационной безопасности	252

ЛЕКЦИЯ XVII	256
Концепция специализированных центров защиты информации	256
Задачи центров защиты информации	257
Функции центров защиты информации	259
Принципы построения центров защиты информации	260
Автоматизированная сеть центров защиты информации	261
Формирование баз данных как основная задача центров защиты информации	265
ЛЕКЦИЯ XVIII	272
Развитие подготовки специалистов в области обеспечения информационной безопасности	272
Анализ современного состояния системы подготовки кадров	273
Дополнительное профессиональное образование	276
Потребность в специалистах в области обеспечения информационной безопасности	277
Концепция межведомственной системы подготовки и переподготовки кадров в области обеспечения информационной безопасности	281
Требования к содержанию подготовки специалистов в области обеспечения информационной безопасности	285
Итоги раздела 6	287
Выводы по материалам раздела 6	287
Вопросы для повторения	289
Послесловие	290
Рекомендуемая литература	292
Основная литература	292
Дополнительная литература	293
Научно-технические журналы	293
Задания для самостоятельной работы	295

Приложение. АВТОМАТИЗИРОВАННАЯ СИСТЕМА	
«ЭКСПЕРТ-ЗАЩИТА»	298
Назначение и общая структура системы	298
Подсистема «Подготовка экспертов»	299
Подсистема «Работа экспертов»	300
Подсистема «Обработка экспертных оценок»	304
Структура «Базы данных»	305