

Оглавление

Список основных сокращений

Предисловие

ЛЕКЦИЯ I

Введение

Наиболее острые проблемы сегодняшнего дня

Исторический очерк

Содержание курса

РАЗДЕЛ 1

СОВРЕМЕННЫЕ ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

ЛЕКЦИЯ II.

Определение понятия «Информационная безопасность»

Общая схема обеспечения информационной безопасности

Проблема защиты информации

Анализ развития подходов к защите информации

Эмпирический, концептуально-эмпирический и теоретико-концептуальный подходы

ЛЕКЦИЯ III

Современная постановка задачи защиты информации

Основные факторы современного этапа

Основные концептуальные положения

Переход к интенсивным способам защиты информации

Кортеж концептуальных решений

Формирование баз исходных данных

Итоги раздела 1

Выводы по материалам раздела 1

Вопросы для повторения

РАЗДЕЛ 2

НАУЧНО-МЕТОДОЛОГИЧЕСКИЕ ОСНОВЫ ИНТЕНСИФИКАЦИИ ПРОЦЕССОВ ЗАЩИТЫ ИНФОРМАЦИИ

ЛЕКЦИЯ IV

Определение и принципы формирования теории защиты информации

Общетеоретические принципы формирования теории

Теоретико-прикладные принципы

Методологический базис теории защиты информации

Методы теории нечетких множеств

Методы теории лингвистических переменных

Неформальные методы оценивания

Неформальные методы поиска оптимальных решений

ЛЕКЦИЯ V

Развитие неформальных методов анализа процессов защиты информации. Автоформализация знаний эксперта

Структура процесса принятия решений

Формирование базы данных

Формирование базы моделей

Принципы построения модели защиты от несанкционированного доступа

Монитор обращений

Правила разграничения доступа

Вербальная модель разграничения доступа

Модель Хартсона

Модель Лэмпсона, Грэхема, Деннинга

Модель Белла и Ла Падула

ЛЕКЦИЯ VI

Обобщенная модель процессов защиты информации
Энтропийный подход к моделированию
Модель системы обеспечения безопасности информации

ЛЕКЦИЯ VII

Основное содержание теории защиты информации
Стратегии защиты информации
Унифицированная технология автоматизированной обработки информации
Унифицированная концепция защиты информации
Итоги раздела 2
Выводы по материалам раздела 2
Вопросы для повторения

РАЗДЕЛ 3 МЕТОДОЛОГИЯ ОЦЕНКИ УЯЗВИМОСТИ ИНФОРМАЦИИ

ЛЕКЦИЯ VIII

Понятие угрозы безопасности информации
Подходы к классификации угроз
Системная классификация угроз
Показатели уязвимости информации
Базовый, обобщенный, общий и экстремальные показатели уязвимости
Учет интервала времени оценки

ЛЕКЦИЯ IX

Оценка достоверности информационной базы прогнозирования показателей уязвимости информации
Модификация фрагментов интегрированной базы данных
Методы обработки свидетельств
Применение методов фильтрации
Алгоритм оптимального фильтра Калмана

ЛЕКЦИЯ X

Понятие информационного риска
Модели оценки вероятности проявления угроз безопасности
Модели оценки ущерба от реализации угроз безопасности информации
Динамическая модель оценки потенциальных угроз
Модель оценки ущерба в терминах теории игр
Выводы по рассмотренным моделям
Итоги раздела 3.
Выводы по материалам раздела 3
Вопросы для повторения

РАЗДЕЛ 4 МЕТОДОЛОГИЯ ОПРЕДЕЛЕНИЯ ТРЕБОВАНИЙ К ЗАЩИТЕ ИНФОРМАЦИИ

ЛЕКЦИЯ XI

Постановка задачи определения требований к защите информации
Методики определения требований к защите
Основные действующие документы Российской Федерации
Анализ применяемых методик
Подходы к преодолению недостатков действующих методик
Определение параметров защищаемой информации
Важность информации
Полнота информации
Адекватность информации
Релевантность информации
Тolerантность информации.
Оценка информации как объекта труда

ЛЕКЦИЯ XII

Оценка факторов, влияющих на требуемый уровень защиты
Формирование множества факторов
Определение весов и классификация вариантов потенциально возможных условий защиты информации
Использование методов кластерного анализа
Эмпирический подход к делению на классы
Итоги раздела 4
Выводы по материалам раздела 4
Вопросы для повторения

РАЗДЕЛ 5 МЕТОДОЛОГИЯ ФОРМИРОВАНИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

ЛЕКЦИЯ XIII

Определение системы защиты информации
Типизация и стандартизация систем защиты информации
Высший уровень типизации и стандартизации
Средний уровень типизации и стандартизации
Низший уровень типизации и стандартизации
Адаптация и управление развитием систем защиты информации
Многокритериальный развивающийся объект
Монотонный критерий
Формализация политики безопасности
Оценка эффективности процессов защиты

ЛЕКЦИЯ XIV

Общая модель управления системой защиты
Основные макропроцессы управления
Методологические основы выработки управленческих решений
Особенности многокритериальных задач управления
Контроль защищенности информации

ЛЕКЦИЯ XV

Комплексная политика защиты информации
Функции защиты
Задачи защиты
Средства и методы защиты
Система защиты информации
Итоги раздела 5
Выводы по материалам раздела 5
Вопросы для повторения

РАЗДЕЛ 6 ПЕРСПЕКТИВЫ РАЗВИТИЯ ТЕОРИИ И ПРАКТИКИ ЗАЩИТЫ ИНФОРМАЦИИ

ЛЕКЦИЯ XVI

Анализ гносеологии развития теории защиты информации
Совершенствование теоретических основ защиты информации
Перевод защиты информации на индустриальную основу
Расширение постановки задачи защиты. Обеспечение информационной безопасности

ЛЕКЦИЯ XVII

Концепция специализированных центров защиты информации
Задачи центров защиты информации
Функции центров защиты информации
Принципы построения центров защиты информации
Автоматизированная сеть центров защиты информации
Формирование баз данных как основная задача центров защиты информации

ЛЕКЦИЯ XVIII

Развитие подготовки специалистов в области обеспечения информационной безопасности

Анализ современного состояния системы подготовки кадров
Дополнительное профессиональное образование
Потребность в специалистах в области обеспечения информационной безопасности
Концепция межведомственной системы подготовки и переподготовки кадров в области обеспечения информационной безопасности
Требования к содержанию подготовки специалистов в области обеспечения информационной безопасности
Итоги раздела 6
Выводы по материалам раздела 6
Вопросы для повторения
Послесловие
Рекомендуемая литература
Основная литература
Дополнительная литература
Научно-технические журналы
Задания для самостоятельной работы

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