МИНОБРНАУКИ РОССИИ

Государственное образовательное учреждение высшего профессионального образования

**«Санкт-Петербургский государственный электротехнический**

**университет “ЛЭТИ” им.В.И. Ульянова (Ленина)»**

**(СПбГЭТУ)**

“УТВЕРЖДАЮ”

проректор по учебной работе

проф.\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Лысенко Н.В.

"\_\_\_\_\_\_"\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2011.г.

ПРОГРАММА

**ГОСУДАРСТВЕННОГО МЕЖДИСЦИПЛИНАРНОГО ЭКЗАМЕНА**

Для подготовки дипломированных специалистов по специальности

090102.65«Компьютерная безопасность»

Факультет компьютерных технологий и информатики

Выпускающая кафедра автоматизированных систем обработки информации и управления

# Санкт-Петербург

2011

Программа государственного междисциплинарного экзамена составлена в соответствии с государственным образовательным стандартом для подготовки дипломированных специалистов по специальности 090102.65 — «Компьютерная безопасность»*,*а также на основании «Положения об итоговой государственной аттестации выпускников СПбГЭТУ «ЛЭТИ».

1. В основу программы положены следующие дисциплины базовой и вариативной частей математического и естественнонаучного, а также профессионального циклов подготовки специалистов по специальности 090102.65 — «Компьютерная безопасность»

**Модульдисциплин направления**

**ЕН:**

1. Теория информационных процессов и систем
2. Теория принятия решений

**ДС:**

1. Теоретико-числовые методы в криптографии
2. Защита ОС и СУБД

**ОПД:**

1. Архитектура современных ЭВМ и системное ПО
2. Системы реального времени
3. Сети ЭВМ и телекоммуникации
4. Технические средства и методы защиты информации
5. Криптографические методы защиты информации

2. Выпускники должны:

**Знать:** принципы, методы, средства, технологии защиты компьютерных систем от угроз; разработка, внедрение, сопровождение информационных систем в защищенном исполнении; политики и профили безопасности.

3. Программа государственного междисциплинарного экзамена включает в себя следующие основные разделы дисциплин:

1. *Теория информационных процессов и систем*

* Понятие информации. Количество информации в равновероятных и неравновероятных сообщениях
* Энтропия дискретных событий. Виды энтропии.
* Взаимная информация. Энтропия источника и энтропия событий.
* Энтропия непрерывных сообщений (свойства).
* Понятие и типы каналов связи.
* Модель и характеристика непрерывных каналов связи.
* Классификация и модели дискретного канала связи.
* Скорость передачи информации и пропускная способность в дискретном канале связи без шума и с шумом.
* Кодирование дискретной информации в канале связи без шума (процедуры Шеннона и Хаффмана).
* Прямая теорема Шеннона для дискретного канала связи с шумом.
* Понятие и типы кодов. Геометрические модели кодов.
* Методика построения линейных систематических кодов (образующая матрица). Процедура декодирования линейных кодов.
* Коды Хемминга. Коды Хемминга с проверкой на четность.
* Модель ошибки в дискретном канале связи без памяти. Информационный предел избыточности для дискретного канала связи без памяти.
* Модели ошибки в дискретном канале связи с памятью. Минимальная избыточность для обнаружения и исправления ошибок в дискретном канале связи с памятью.
* Обратная теорема Шеннона. Эквивалентная вероятность ошибки.
* Циклические коды. Процедуры кодирования и декодирования.
* Понятие и свойства непрерывных кодов.
* Построение оптимальной шкалы квантования. Поэлементный метод приема сигналов. Методы приема сигнала в целом.
* Система с обратной связью.

1. *Теория принятия решений*

* Принципы, методы и средства исследования операций. Понятие рациональности и эффективности. Их соотношение. Понятие системы. Сложные системы. Системный анализ и исследование операций. Понятие организации, анализ организации, информационные модели.
* Операционный подход к задачам принятия решений, отличительные особенности. Характеристики задач исследования операций. Содержание и формы задачи. Системный подход к задачам принятия решений, комплексный подход. Постановка задачи исследования операций, элементы задачи, исследовательская задача.
* Качественные факторы в задачах принятия решений. Экспертное оценивание. Экспертное оценивание, методы дискуссии, суда, метод Делфи, метод последовательных сопоставлений оценок.
* Многокритериальная оптимизация, основные проблемы, классы задач. Паретооптимальные решения. Метод свертки критерия. Методы уступок. Методы равенства. Метод главного критерия. Метод идеальной точки. Оптимизация по последовательно применяемым критериям.
* Целочисленное линейное программирование, особенности задач, методы отсечения. Дискретный алгоритм, смешанный алгоритм, циклический алгоритм. Метод ветвей и границ, общая схема. Решение линейных целочисленных задач. Задача о коммивояжере.
* Динамическое программирование, принцип Белмана, схема метода. Задача распределения капиталовложений. Задача о замене оборудования. Задача о садовнике. Задача управления запасами. Марковские процессы принятия решений. Вложенная задача распределения ресурсов. Задача о рекламе. Задача о рюкзаке.
* Системы массового обслуживания. Классификация систем, основные характеристики. Основные элементы системы. Входящий поток требований. Механизмы обслуживания. Дисциплины обслуживания: СМО без очереди, с неограниченной очередью, с ограниченной очередью, замкнутые, с неодинаковыми приборами, с приоритетами, многофазные, упорядоченные.
* Анализ конфликтных ситуаций. Основные понятия теории игр. Матричные игры с седловой точкой. Оптимальные стратегии. Смешанные стратегии. Основная теорема теории игр. Свойства оптимальных стратегий. Решение матричных игр.

1. *Архитектура современных ЭВМ и системное ПО*

* Аппаратные средства IBM PC.
* Архитектура MS DOS.
* Файловая система FAT.
* Прерывания, вектора прерываний.
* Видеоподсистема и ее характеристики, типы видеоадаптеров.
* Видеокарта, структура.
* Клавиатура.
* Порты ввода-вывода. Параллельный порт.
* Порты ввода-вывода. Последовательный порт.
* Печатающие устройства. Шрифты.
* Архитектура 8086.
* Архитектура 80386. Системные регистры.
* 80386 – работа с сегментами. Дескриптор сегментов.
* 80386 – уровни защиты, переход между уровнями.
* Система команд 386-486 процессоров.
* 80386 – виртуальная память.
* Арифметические сопроцессоры.
* ОС UNIX. Файловая система.
* Процессы и их типы.
* Процессы, порождения процессов.
* Взаимодействия процессов. Сигналы.
* Взаимодействия процессов. Каналы.
* Взаимодействия процессов. Сообщения.
* Взаимодействия процессов. Разделяемая память.
* Взаимодействия процессов. Семафоры.
* Система ввода-вывода. Драйвера.
* Планирование процессов.
* ОС реального времени.
* Методы оценки производительности систем.

1. *Системы реального времени*

* Особенности СРВ, характеристики, ограничения «жесткого» и «мягкого» реального времени.
* Архитектура СРВ, средства взаимодействия с внешней средой.
* Интерфейсы последовательной связи.
* Приборный интерфейс.
* Магистрально-модульные интерфейсы.
* Операционные системы реального времени (RTOS), особенности архитектуры.
* Многозадачность RTOS; создание задачи, управление задачами.
* Стандарты POSIX для систем реального времени.
* Проблема инверсии приоритетов, способы решения.
* Приоритетное планирование задач. Статические алгоритмы. Дисциплина RateMonotonic.
* Динамические алгоритмы планирования.
* Синхронизация процессов, проблема тупиков.
* Механизм семафоров.
* Задача «Поставщик – потребитель».
* Реализация механизма семафоров.
* Mutualexclusion, реализация mutex.
* Монитор, механизм сигналов.
* Задача «Читатели – писатели».
* Задачи в языке АДА, механизм рандеву.
* Реализация механизма семафоров и механизма сигналов через рандеву.
* Задача «Поставщик – потребитель» и отбор среди входов.
* Особенности языков программирования реального времени.

1. *Сети ЭВМ и телекоммуникация*

* Область использования информационных сетей. Производительность. Индексы производительности.
* Общие ресурсы информационных сетей. Понятие сервера. Принципы организации и доступа. Типы серверов.
* Методы доступа в среду передачи данных. Временная и пространственная селекция. Адресация и идентификация в сетях. Синхронизация в информационных сетях.
* Модель информационной сети. Принципы многоуровневой организации Протоколы взаимодействия на различных уровнях. Иерархия представления данных.
* Средства аппаратной поддержки информационных сетей. Конфигурации локальных сетей. Принципы объединения локальных сетей.
* Использование возможностей систем телекоммуникаций для организации единого информационного пространства и доступа к общим ресурсам.
* Администрирование и управление информационными сетями. Проблемы передачи сообщений на сетевом и транспортном уровнях. Маршрутизация потоков в информационных сетях.
* Организация доступа в системы телекоммуникаций. Аппаратная поддержка доступа. Адаптеры. Модемы. Протоколы взаимодействия.
* Защита информации в информационных сетях. Уровни защиты. Криптография.
* Контроль на транспортном и сеансовом уровнях. Методы и средства повышения безопасности информационных сетей.
* Распределенные системы обработки данных (РСОД) и информационные технологии (ИТ).
* Информационные процессы современного предприятия. Офисный и технический документооборот.
* Корпоративные информационные системы (КИнС).
* Методы и средства проектирования информационных систем. Традиционные методы проектирования КинС.
* CASE-средства и технологии проектирования РСОД.
* Проблемы разработки РСОД. Задачи интеграции в гетерогенной информационной среде.
* Сети Петри как аппарат исследования РСОД. Методы анализа сетей Петри. Синтез структуры централизованных РСОД. Синтез структуры древовидных РСОД.
* Характеристика трафика в распределенных автоматизированных системах.
* Алгоритмы управления информационными потоками и выбор стратегии маршрутизации в РСОД.
* Проблемы, особенности и постановка задачи управления доставкой информации в РСОД.

1. *Технические средства и методы защиты информации*

* Информация, как объект защиты. Виды, источники и носители защищаемой информации.
* Обобщенная модель технического канала утечки информации. Классификация и основные характеристики технических каналов утечки информации.
* Классификация технической разведки. Возможности видов технической разведки.
* Источники опасного сигнала. Демаскирующие признаки объектов наблюдения и сигналов.
* Побочные электромагнитные излучения и наводки. Зоны пространственной защиты информации от утечки за счет побочных излучений.
* Побочные электромагнитные излучения и наводки. Методы защиты информации от утечки за счет побочных излучений и наводок.
* Побочные электромагнитные излучения и наводки. Защита информации на объектах информатизации.
* Защита речевой информации от утечки по атмосферному, виброакустическому и оптикоэлектронному каналам.
* Сокрытие речевой информации в каналах связи.
* Классификация технической разведки. Характеристика государственной системы противодействия технической разведке.
* Организация защиты информации. Структура государственной системы защиты информации.
* Мероприятия по защите информации. Лицензирование в области защиты информации. Аттестация объектов.
* Мероприятия по защите информации. Сертификация средств защиты информации. Категорирование защищаемой информации.
* Мероприятия по контролю эффективности защиты информации. Организационный и технический контроль.
* Специальная проверка объектов. Обнаружение и локализация закладных устройств, подавление их сигналов.
* Специальная проверка объектов. Средства перехвата информации с передачей ее по радиоканалу.
* Специальная проверка объектов. Средства перехвата информации с передачей ее по проводным линиям.
* Содержание специальной проверки объектов, ее основные технологические процедуры.

1. *Криптографические методы защиты информации*

* Задачи защиты информации, решаемые с использованием криптографических методов: аутентификация субъектов и информации, обеспечение секретности и анонимности. Методы аутентификации пользователей. Слабая и сильная аутентификация. Схема парольного контроля доступа входа в компьютерную систему. Протокол рукопожатия (аутентификация удаленных пользователей). Безконтактная аутентификация. Протоколы с нулевым разглашением.
* Построение криптографических временных замков.
* Аутентификация информации в системах с арбитром и системах с судьей. Системы электронной цифровой подписи (ЭЦП). Криптосистема RSA. Системы ЭЦП на основе сложности задачи дискретного логарифмирования по большому простому модулю. Системы ЭЦП на основе арифметических вычислений по составному модулю. Схемы ЭЦП с сокращенной длиной подписи. Защита материальных объектов от подделки с использованием ЭЦП. Удостоверяющие центры. Инфраструктура открытых ключей. Цифровые сертификаты. Виды атак на системы ЭЦП. Слепая подпись Чаума.
* Виды атак на симметричные шифры. Частотныйкриптоанализ подстановочных шифров. Дифференциальный и линейный криптоанализ. Схемы и принципы построения блочных криптографических алгоритмов. КриптосхемаФейстеля как суперпозиция инволюций. Расписание использования ключа. Итеративные шифры. Режимы использования блочных шифров. Поточные и адитивные шифры. Варианты реализации шифров. Обобщения криптосхемыФейстеля. Блочные шифры RC5, Blowfish и RC6. Программные шифры на основе выборки подключей в зависимости от преобразуемых данных. Технологическая роль шифрования в современных системах защиты информации. Влияние технологических факторов на выбор механизма криптографического преобразования. Недетерминированные шифры как криптосистемы с предвычислениями. Схемы блочных шифров на основе управляемых подстановочно-перестановочных сетей (УППС). Выбор управляемых элементов для построения УППС. Конструктивные критерии. Стандарты шифрования: DES, AES и ГОСТ 28147-89.Роль стандартов в повышении эффективности средств защиты информации. Проблема доверия пользователей. Стойкость и потайные лазейки. Режимы использования блочных шифров.
* Вероятностное шифрование в симметричных и асимметричных криптосистемах. Монофонические шифры.
* Методы контроля целостности информации. Алгоритмы защитного контрольного суммирования с ключом и без ключа. Схемы построения стойких хэш-функций на основе блочных шифров. Хэш-функции на основе арифметических вычислений. Хэш-функции с секретом и их применение.
* Управление ключами в симметричных криптосистемах: генерация, распространение, хранение и уничтожение ключей. Централизованное и децентрализованное распределение ключей. Иерархия ключей. Факторы, определяющие срок действия ключей. Неоднородное ключевое пространство. Депонирование ключей. Схемы разделения секрета.

1. *Теоретико-числовые методы в криптографии*

* Характер криптографической деятельности. Криптография и стеганография. Понятие о ключе и шифре. Криптографическая стойкость шифров. Простейшие шифры и их свойства. Подстановочно-перестановочные шифры. Основные требования к шифрам. Принцип Керхкоффа. Теоретико-информационный подход к оценке стойкости шифров. Условная и безусловная стойкость. Теоретическая и практическая стойкость. Проблема распределения секретных ключей. Понятие о криптоанализе.
* Секретность алгоритма шифрования и стойкость (практическая и теоретическая). Вычислительно стойкие шифры. Проблема оценки стойкости. Базовые принципы разработки шифров. Рассеивание и перемешивание. Лавинный эффект. Блочные шифры.
* Вероятностное шифрование как способ повышения стойкости шифрования. Достоинства и недостатки вероятностного шифрования. Вопросы контроля целостности информации. Хэш-функции. Стойкость хэш-функций. Хэш-функция как составной элемент систем электронной цифровой подписи. Выбор длины хэш-кода и парадокс дней рождения.
* Новые примитивы симметричного шифрования – переменные операции перестановочного и подстановочного типа. Булевы функции в анализе примитивов и шифров. Управляемые подстановочно-перестановочные сети как криптографический примитив.
* Элементы теории чисел: сравнения, функция Эйлера, теоремы Ферма и Эйлера, Алгоритм быстрого возведения в большую дискретную степень, обратный элемент в поле вычетов по простому модулю, расширенный алгоритм Евклида. Показатели по модулю. Первообразный корень. Нахождение чисел, относящихся к заданному простому и составному показателям. Дискретный логарифм. Вычисление функции Эйлера. Задача разложения числа на два больших простых делителя. Генерация простых и псевдопростых чисел. Тесты Ферма и Соловея-Штрассена. Понятие односторонней функции. Метод открытого распределения ключей Диффи-Хелмана. Идея электронной цифровой подписи. Открытый и закрытый ключ. Проблема аутентификации открытых ключей. Каналы распределения открытых ключей. Понятие криптографического протокола. Системы ЭЦП на основе сложности задачи дискретного логарифмирования. Открытое шифрование методом Эль-Гамаля и его связь с методом Диффи-Хеллмана.
* Проблема распространения секретных ключей. Использование двухключевых криптосистем для распределения ключей в симметричных криптосистемах. Гибридные криптосистемы. Проблема аутентификации открытых ключей в двухключевых криптосистемах.

1. *Защита ОС и СУБД*

* Понятие национальной безопасности: виды безопасности: государственная, экономическая, общественная, военная, экологическая, информационная; роль и место системы обеспечения информационной безопасности (ИБ) в системе национальной безопасности РФ; доктрина ИБ, история проблемы ИБ, угрозы ИБ; методы и средства обеспечения ИБ; методологические и технологические основы комплексного обеспечения ИБ; модели, стратегии и системы обеспечения ИБ; методы управления, организации и обеспечения работ по обеспечению ИБ; обеспечение ИБ в нормальных и чрезвычайных ситуациях; проблемы информационной войны; правовые и нормативные акты в области ИБ.
* Законодательство РФ в области информационной безопасности, защиты государственной тайны и конфиденциальной информации; конституционные гарантии прав граждан на информацию и механизм их реализации; понятие и виды защищаемой информации по законодательству РФ; защита интеллектуальной собственности средствами патентного и авторского права; правовая регламентация охранной деятельности; международное законодательство в области защиты информации.
* Анализ и оценка угроз информационной безопасности объекта; оценка ущерба вследствие противоправного раскрытия информации ограниченного доступа и меры по его локализации; средства и методы физической защиты объектов; системы сигнализации, видеонаблюдения, контроля доступа; служба безопасности объекта; подбор, расстановка и работа с кадрами; организация и обеспечение режима секретности; организация пропускного и внутриобъектового режима; организация режима и охраны объектов в процессе транспортировки; защита информации при авариях, иных экстремальных ситуациях и в условиях чрезвычайного положения; технологические меры поддержания информационной безопасности объектов; обеспечение информационной безопасности объекта (учреждения, банка, промышленного предприятия) при осуществлении международного научно-технического и экономического сотрудничества.
* Общие вопросы организации противодействия технической разведке; основные организационные и технические мероприятия, используемые для противодействия технической разведке; методы и средства защиты режимных объектов от утечки конфиденциальной информации по техническим каналам; физические основы образования побочных электромагнитных излучений от технических средств; каналы утечки информации: электромагнитные, электрические (проводные), виброакустические; защита технических средств от утечки информации по этим каналам;нормы эффективности защиты; роль и место технического контроля эффективности защиты информации; нормы, руководящие документы по организации и ведению контроля; организационный и технический контроль; методы контроля; особенности контроля объектов в различных сферах; аппаратура контроля; взаимодействие контрольных органов с подразделениями контроля на местах; методологические основы автоматизации технического контроля; основные задачи технического контроля, требующие автоматизированного решения.
* Структура и принципы функционирования современных вычислительных систем. Проблемы обеспечения безопасности обработки и хранения информации в вычислительных системах. Базовые этапы построения системы комплексной защиты вычислительных систем. Анализ моделей нарушителя. Угрозы информационно-программному обеспечению вычислительных систем и их классификация. Функции системы защиты по предупреждению угроз и устранению последствий их реализации. Классификация способов и средств комплексной защиты информации. Классификация методов защиты информации с использованием программно-аппаратных средств вычислительной системы. Организационная структура системы комплексной защиты информационно-программного обеспечения. Управление системой защиты. Функции ядра системы комплексной защиты. Многоуровневая структура системы защиты на основе программно-аппаратных средств вычислительной системы. Стандарты по оценке безопасности вычислительных систем. Требования руководящих документов Гостехкомиссии.
* Идентификация пользователей и установление их подлинности при доступе к компьютерным ресурсам. Основные этапы допуска к ресурсам вычислительной системы. Использование простого пароля. Использование динамически изменяющегося пароля. Взаимная проверка подлинности и другие случаи опознания. Способы разграничения доступа к компьютерным ресурсам. Разграничение доступа по спискам. Использование матрицы установления полномочий. Произвольное и принудительное управление доступом. Разграничение доступа по уровням секретности и категориям. Понятие меток безопасности. Управление метками безопасности. Парольное разграничение доступа и комбинированные методы. Особенности программной реализации контроля установленных полномочий. Защита программных средств от несанкционированного копирования, исследования и модификации. Привязка программ к среде функционирования. Защита программ от несанкционированного запуска.
* История появления компьютерных вирусов и факторы, влияющие на их распространение. Понятие компьютерного вируса. Основные этапы жизненного цикла вирусов. Объекты внедрения, режимы функционирования и специальные функции вирусов. Схемы заражения файлов. Схемы заражения загрузчиков. Способы маскировки, используемые вирусами. Классификация компьютерных вирусов. Общая организация защиты от компьютерных вирусов. Транзитный и динамический режимы антивирусной защиты. Поиск вирусов по сигнатурам и обезвреживание обнаруженных вирусов. Углубленный анализ на наличие вирусов путем контроля эталонного состояния компьютерной системы. Защита от деструктивных действий и размножения вирусов. Использование средств аппаратного и программного контроля. Стратегия заблаговременной подготовки к эффективной ликвидации последствий вирусной эпидемии. Технология гарантированного восстановление вычислительной системы после заражения компьютерными вирусами.
* Введение в криптографию. Представление защищаемой информации; угрозы безопасности информации; ценность информации; основные термины и понятия криптографии; открытые сообщения и их характеристики; модели открытых сообщений; исторический очерк развития криптографии; Типы криптографических систем. Простые методы шифрования: шифры подстановки и перестановки. Подстановки с переменным коэффициентом сдвига. Многослойные шифры. Использование псевдослучайных чисел для генерации ключей. Выбор порождающего числа и максимизация длины последовательности чисел ключа. Режимы шифрования. Особенности шифрования данных в режиме реального времени. Шифрование ключа при необходимости его хранения с зашифрованными данными. Скоростные и недетерминированные программные шифры. Основы скоростного шифрования. Внесение неопределенностей в процесс криптографических преобразований. Стандарты шифрования. Протоколы распределения ключей; протоколы установления подлинности; электронная цифровая подпись; Общая организация криптографической защиты информации. Использование общесистемных и специализированных программных средств для шифрования файлов и работы с секретными внешними носителями информации.
* Введение в проблему. Виды остаточных данных. Способы защиты от несанкционированного использования остаточной информации. Использование специализированных программ по уничтожению остаточных данных. Специальные режимы и особенности шифрования данных в режиме реального времени с возможность мгновенного уничтожения данных. Использование общесистемных и специализированных программных средств для мгновенного уничтожения данных.
* Основные способы защиты от потери информации и нарушений работоспособности вычислительных средств. Внесение функциональной и информационной избыточности. Способы резервирования информации. Правила обновления резервных данных. Методы сжатия информации. Архивация файловых данных. Особенности архивации на магнитные диски и магнитную ленту. Резервирование системных данных. Подготовка программных средств восстановления. Безопасная инсталляция программных средств. Общие сведения о нарушении доступа к дисковой и оперативной памяти. Технология восстановления дисковой и оперативной памяти. Диагностирование и устранение логических и физических дефектов магнитных дисков. Восстановление разметки дискеты и корневого каталога. Отмена результатов форматирования и восстановление поврежденных файлов данных. Защита файлов от удаления и восстановление удаленных файлов. Безопасное кэширование и дефрагментация дисковой памяти. Восстановление и оптимизация оперативной памяти компьютера. Ручное восстановление данных. Безопасное окончание работы на компьютере.
* Общие сведения о реализации защиты информационно-программного обеспечения в операционных системах. Классификация функций защиты по уровням безопасности, поддерживаемых операционной системой (ОС). Ядро безопасности ОС. Аппаратная основа реализации защиты на уровне ОС. Стандарты по оценке уровня безопасности ОС. Внесение функциональной и информационной избыточности ресурсов на уровне ОС. Основы надежного администрирования ОС. Используемые способы разграничения доступа к компьютерным ресурсам, а также службы регистрации и сигнализации. Средства ОС по диагностированию и локализации несанкционированного доступа к ресурсам ВС. Безопасные файловые системы современных ОС (HPFS, NTFS). Подсистемы безопасности современных ОС (Windows 95, Windows NT, UNIX), их недостатки и основные направления совершенствования.
* Концептуальные вопросы построения уровней защиты систем управления базами данных (СУБД). Основные требования к подсистеме безопасности СУБД. Общие сведения о разграничении доступа к базам данных. Обязанности администратора по защите баз данных от несанкционированного доступа. Определение полномочий пользователей по доступу к базе данных. Использование матрицы полномочий для разграничения доступа к элементам баз данных. Мандатная система разграничения доступа. Защита данных при статистической обработке. Общее понятие о целостности базы данных. Типы ошибок, ведущих к нарушению целостности. Задание ограничений целостности. Транзакция и ее свойства. Восстановление базы данных. Особенности восстановления распределенной базы данных. Проблема непротиворечивости при параллельной обработке данных. Использование блокирования для управления параллельной обработкой. Метод независимого выполнения транзакций. Управление параллельными транзакциями на основе временных и версионных отметок. Метод обнаружения противоречивых записей журнала регистрации. Метод использования теста правильности. Разрешение тупиковых ситуаций. Инструментальные средства СУБД по обеспечению целостности баз данных.
* Анализ структуры и принципов функционирования вычислительных сетей с позиции обеспечения информационной безопасности. Угрозы информационно-программному обеспечению, характерные только для распределенной вычислительной среды. Использование криптографических систем для защиты данных, циркулирующих в вычислительной сети. Особенности применения симметрических и асимметрических систем шифрования. Распределение ключей между узлами вычислительной сети. Выработка секретных ключей по Диффи-Хеллману. Распределение ключей с помощью асимметрических систем шифрования. Взаимное подтверждение подлинности при обмене сообщениями в сети. Поддержание целостности циркулирующих в сети сообщений. Формирование и проверка цифровой подписи. Защита от отрицания фактов отправки и приема сообщений. Защита от наблюдения за потоком сообщений (трафиком) в сети. Защита в Internet и Intranet. Использование межсетевых экранов (брандмауэров) для защиты информации в локальных вычислительных сетях. Типы межсетевых экранов, их достоинства и недостатки. Ограничение доступа из локальной сети в Internet с помощью proxy-серверов. Безопасность JAVA-приложений.
* Методы и средства ограничения доступа к компонентам ЭВМ, надежность средств защиты компонент; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям; методы и средства хранения ключевой информации, типовые решения в организации ключевых систем; защита программ от изучения, способы встраивания средств защиты в программное обеспечение; защита от разрушающих программных воздействий (РПВ), понятие изолированной программной среды, защита программ от изменения и контроль целостности; системные вопросы защиты программ и данных, основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности; программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных, вычислительных сетях.

4.Литература

К дисциплине *«Теория информационных процессов и систем»*

1. Колесник В.Д., Полтырев Г.Ш. Курс теории информации. – М.: Наука, 1982. – 416 с.
2. Советов Б.Я. Теория информации. – Л.: изд-во ЛГУ, 1977. – 181 с.
3. Советов Б.Я. Информационная технология. – М.: Высшая школа, 1994. – 368 с.
4. Советов Б.Я., Яковлев С.А. Построение сетей интегрального обслуживания. – Л.: Машиностроение, 1990. – 332 с.
5. Шеннон К. Работы по теории информации и кибернетике. – М.: Изд-во иностранной литературы, 1963. – 830 с.

К дисциплине *«Теория принятия решений»*

1. Вагнер Г. Основы исследования операций: В 3-х томах. – М.: Мир, 1972-1973. Т. 1, 3362 с. Т. 2, 488 с. Т. 3, 504 с.
2. Исследование операций: В 2-х томах. Под ред. Дж. Моудера, С. Элмаграби. – М.: Мир, 1981. Т. 1, 712 с. Т. 2, 677 с.
3. Таха Х. Введение в исследование операций: В 2-х книгах. – М.: Мир, 1985. Кн. 1, 479 с. Кн. 2, 496 с.
4. Дегтярев Ю.И. Методы оптимизации: Учебное пособие для вузов. – М.: Советское радио, 1980. – 272 с.
5. Дегтярев Ю.И. Системный анализ и исследование операций. – М.: Высшая школа, 1997.
6. Реклейтис Г., Рейвиндран А., Рэгсдел К. Оптимизация в технике: В 2-х кн. – М.: Мир, 1986. Кн. 1, 352 с. Кн. 2, 320 с.

К дисциплине *«Архитектура современных ЭВМ и системное ПО»*

1. Скляров В.А. Применение ПЭВМ. Книга 1: Организация и управление ресурсами ПЭВМ. – М.: Высшая школа, 1992.

2. Касаткин А.И., Вальвачев А.Н. Профессиональное программирование на языке СИ. Книги 1, 2, 3. – Минск: Высшая школа, 1993.

3. Гук М. Аппаратные средства IBM PC: Энциклопедия – СПб: Питер Ком, 1999.

К дисциплине *«Системы реального времени»*

1. Сидельников В.В., Широков В.В. Архитектура управляющих систем реального времени. Учебное пособие. – СПб.: ЛЭТИ, 1990
2. Сидельников В.В., Широков В.В. Управление процессами в программных средах АСОИУ. Учебное пособие. – СПб.: ЛЭТИ, 1994
3. Фомичев В.С. Синхронизация вычислительных процессов Учебное пособие. – СПб.: ЛЭТИ, 1990
4. Сидельников В.В., Широков В.В. Модели задач синхронизации в системах реального времени. Методические указания к лабораторным работам по дисциплине «Системы реального времени». – СПб.: ЛЭТИ, 2000

К дисциплине *«Сети ЭВМ и телекоммуникации»*

1. Мизин И.А., Богатырев В.А., Кулешов А.П. Сети коммутации пакетов. – М.: Радио и связь, 1986.
2. Жожикашвили В.А., Вишневский В.Н. Сети массового обслуживания. Теория и применение к сетям ЭВМ. – М.: Радио и связь, 1988.
3. Шварц М. Сети связи: протоколы, моделирование и анализ: В 2-х частях. – М.: Наука, 1992. – 336 с.
4. Советов Б.Я., Яковлев С.А Построение сетей интегрального обслуживания. – СПб.: Машиностроение, 1993. – 332 с.
5. Гавриков А.Л., Постельник Д.Я. Задача синтеза информационной архитектуры сети. // Информационные технологии. – 1997, № 2, с. 33-37.
6. Яковлев С.А. Адаптивное управление процессом обмена информацией в системах автоматизации распределенных производственных объектов. // Известия ЭТУ: Сборник научных трудов. – СПб.: 1994, вып.337, с. 39-44.
7. Арсеньев Б.П., Яковлев С.А. Интеграция распределенных баз данных. – СПб: Издательство «Лань», 2001. – 464 с.
8. Афанасьев А. Методы управления документооборотом в организации// Материалы конф. «Офисные информационные системы-96». – http://www.citforum.ru/koi/ofis/ofis96/104.shtml.
9. Ахметов К. Экономика ИТ и корпоративные информационные системы. // КомпьютерПресс, 1997, № 1, с. 31-33.
10. Биленко А.И., Слипченко Ю.А., Громов А.И. Применение метода имитационного моделирования для оценки параметров функционирования сетей передачи данных. // Механиз. и автоматиз. упр. – 1991, № 3, с. 11-15.
11. Волобуев В. Технология ISDN в информационных сетях. // Сети. – 1997, № 4, с. 14-24.
12. Захаров Г.П., Симонов М.В., Яновский Г.Г. Широкополосные цифровые сети интегрального обслуживания. – СПб.: СПбГУТ, 1996. – 24 с.
13. Лазарев В.Г. Интеллектуальные цифровые сети. – М.: Финансы и статистика, 1996. – 223 с.
14. Информационная технология в промышленности. / Ю.Г. Данилевский, И.А. Петухов, В.С. Шибанов. – Л.: Машиностроение, 1988. – 283 с.
15. Информационное обеспечение интегрированных производственных комплексов. / В.В. Александров, Ю.С. Вишняков, Л.М. Горская и др.; Под ред. В.В. Александрова. – Л.: Машиностроение, 1986. – 264 с.
16. Кумсков М. Унифицированный язык моделирования (UML) и его поддержка в RationalRose 98i – CASE-средстве визуального моделирования // http://www.interface.ru/public/990804/uml4b.htm.
17. Лазарев В.Г., Пийль Е.И. Интеллектуализация телекоммуникационных сетей. // Технологии и средства связи. – 1998, № 2, с. 28-33.
18. Протоколы информационно-вычислительных сетей. / Аничкин С.А., Белов С.А., Бернштейн А.В. и др.; Под ред. Мизина И.А., Кулешова А.П. – М.: Радио и связь, 1990. – 504 с.

К дисциплине *«Технические средства и методы защиты информации»*

1. Анич Б. Защита компьютерной информации. – СПб.: BHV-Питер, 2003.
2. Коул Э. Руководство по защите от хакеров. – М.: Диалектика, 2003.
3. Шиффман М. Защита от хакеров: Анализ 20 сценариев взлома. – М.: Диалектика, 2003.
4. Зима В.М., Молдовян А.А., Молдовян Н.А. Компьютерные сети и защита передаваемой информации. – СПб: издательство СПбГУ, 1998.
5. Зима В.М., Молдовян А.А., Молдовян Н.А. Защита компьютерных ресурсов от несанкционированных действий пользователей: Учебное пособие. – СПб: типография Военной Академии Связи, 1997.
6. Зима В.М., Молдовян А.А. Многоуровневая защита информационно-программного обеспечения вычислительных систем: Учебное пособие. – СПб: СПбГЭТУ «ЛЭТИ», 1997.

К дисциплине *«Криптографические методы защиты информации»*

1. Аграновский А.В. Практическая криптография: алгоритмы и их программирование (+CD). – М.: Солон, 2003.
2. Столлингс В. Криптография и защита сетей: Принципы и практика (2-е издание). – М.: Диалектика, 2003.
3. Шнайер Б. Прикладная криптография: Протоколы, алгоритмы, исходные тексты на языке C. – М.: Триумф, 2003.
4. Молдовян А.А., Молдовян Н.А. Криптография: скоростные шифры. – СПб.: BHV-Питер, 2002.
5. Молдовян Н.А., Молдовян А.А., Еремеев М.А. Криптография: От примитивов к синтезу алгоритмов. – СПб: БХВ-Петербург, 2004. – 456 с.
6. Молдовян А.А., Молдовян Н.А., Советов Б.Я. Скоростные программные шифры и средства защиты информации в компьютерных системах. – СПб: типография Военной Академии связи, 1997.

К дисциплине *«Теоретико-числовые методы в криптографии»*

1. Бабаш А.В. Криптография. – М.: Солон, 2003.
2. Баричев С.Г. Основы современной криптографии: Учебный курс. – М.: Бином, 2003.
3. Барнет С. Криптография: Официальное руководство RSA Security. – М.: Бином, 2003.
4. Молдовян А. Криптография. – СПб.: Лань, 2003.

К дисциплине *«Защита ОС и СУБД»*

1. Вус М.А., Долгирев Д.В., Гусев В.С., Молдовян А.А. Информатика: введение в информационную безопасность.
2. Герасименко В.А. Защита информации в автоматизированных системах обработки данных: В 2-х книгах. – М.: Энергоатомиздат, 1994.
3. Герасименко В.А., Малюк А.А. Основы защиты информации. – М.: МИФИ, 1997.
4. Домарев В.В. Защита информации и безопасность компьютерных систем. – К.: ДиаСофт, 1999.
5. Зима В.М., Молдовян А.А. Многоуровневая защита информационно-программного обеспечения вычислительных систем: Учебное пособие. – СПб: СПбГЭТУ «ЛЭТИ», 1997.
6. Зима В.М., Молдовян А.А. Многоуровневая защита от компьютерных вирусов: Учебное пособие. – СПб: СПбГЭТУ «ЛЭТИ», 1997.
7. Зима В.М., Молдовян А.А. Технология практического обеспечения информационной безопасности: Учебное пособие. – СПб: СПбГЭТУ «ЛЭТИ», 1997.
8. Зима В.М., Молдовян А.А., Молдовян Н.А. Безопасность глобальных сетевых технологий. – СПб: БХВ-Петербург, 2001. – 368 с.
9. Зима В.М., Молдовян А.А., Молдовян Н.А. Защита компьютерных ресурсов от несанкционированных действий пользователей: Учебное пособие. – СПб: типография Военной Академии Связи, 1997.
10. Зима В.М., Молдовян А.А., Молдовян Н.А. Компьютерные сети и защита передаваемой информации. – СПб: издательство СПбГУ, 1998.
11. Зима В.М., Молдовян А.А., Молдовян Н.А. Основы резервирования информации и архивация файловых данных в вычислительных системах: Учебное пособие. – СПб: издательство СПбГУ, 1998.
12. Мафтик С. Механизмы защиты в сетях ЭВМ: Пер. с англ. – М.: Мир, 1993.
13. Мельников В.В. Защита информации в компьютерных системах. – М.: Финансы и статистика; Электронинформ, 1997.
14. Молдовян А.А., Молдовян Н.А., Гуц Н.Д., Изотов Б.В. Криптография: Скоростные шифры. - СПб: БХВ-Петербург, 2003. – 468 с.
15. Молдовян Н.А., Молдовян А.А., Еремеев М.А. Криптография: От примитивов к синтезу алгоритмов. – СПб: БХВ-Петербург, 2004. – 456 с.
16. Молдовян А.А., Молдовян Н.А., Советов Б.Я. Скоростные программные шифры и средства защиты информации в компьютерных системах. – СПб: типография Военной Академии связи, 1997.
17. Молдовян А.А., Молдовян Н.А., Советов Б.Я. Криптография. – СПб.: Лань, 2000.
18. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – М.: Радио и связь, 1999.
19. Феденко Б.А., Макаров И.В. Безопасность сетевых ОС. – М.: ЭКО-ТРЕНДЗ, 1999.
20. Энциклопедия промышленного шпионажа. / Под ред. Е.В. Куренкова. – СПб.: ООО «Издательство Полигон», 1999.

Нормативные документы:

1. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования.
2. ГОСТ 34.10-94. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма.
3. Руководящий документ Гостехкомиссии России. Термины и определения в области защиты от НСД к информации. М.: ГТК РФ, 1992.
4. Руководящий документ Гостехкомиссии России. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. М.: ГТК РФ, 1992.
5. Руководящий документ Гостехкомиссии России. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности СВТ от НСД к информации. М.:ГТК РФ, 1992.
6. Руководящий документ Гостехкомиссии России. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. М.: ГТК РФ, 1992.

Программа одобрена методической комиссией факультета компьютерных технологий и информатики «\_\_\_\_» \_\_\_\_\_ 2011 г, протокол № \_\_\_\_\_\_\_\_\_

Председатель методической комиссии факультета

компьютерных технологий и информатики

к.т.н., доцент Михалков В.А.

Согласовано

Зав. кафедрой автоматизированных систем

обработки информации и управления

д.т.н., профессор Советов Б.Я.