

ПРОГРАММА ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ ПО КОНКУРСНОЙ ГРУППЕ «ФРКТ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ»

ДЛЯ ПОСТУПАЮЩИХ В АСПИРАНТУРУ

Билет включает 2 вопроса. Первый вопрос - из раздела программы, соответствующего направленности, по которой поступающий намерен обучаться. Второй вопрос - по будущей диссертационной работе поступающего: тематика, имеющийся задел, наличие научного руководителя, публикаций. Могут быть также заданы вопросы по содержанию выпускной квалификационной работы (магистра, специалиста).

На подготовку дается 1 час, при этом разрешено пользоваться литературой за исключением электронных носителей. Не разрешается использование средств связи и доступа в интернет. Поступающий отвечает по билету в форме устного собеседования, в ходе которого могут быть заданы дополнительные вопросы по соответствующему разделу программы.

Раздел «Вычислительные системы и их элементы»

1. Первые МП, CISC, RISC и postRISC архитектуры. Структура микропроцессоров различных архитектурных платформ. Характеристики микропроцессоров.
2. Организация конвейера в CISC - микропроцессорах, простых RISC – микропроцессорах, суперскалярных и VLIW – микропроцессорах.
3. Основные группы команд в системах команд МП. Режимы адресации. Формат и размер команд.
4. Конвейерная выборка команд. Кэш команд, трассе кэш, предподкачка команд.
5. Обработка переходов. Предсказание переходов.
6. Группирование команд в суперскалярных МП. Переименование регистров в суперскалярных МП.
7. Элементы управления в конвейерных структурах с динамическим планированием потока команд (scoreboarding, reservation station, reorder buffer).
8. Отложенная запись и bypass в RISC МП.
9. Иерархия памяти Кэш-память данных первого, второго (третьего) уровня.
10. Поддержка работы с виртуальной памятью.
11. Механизмы поддержания когерентности в иерархии памяти.
12. Организация основной памяти.
13. Структура внешнего интерфейса МП. Шины. Кольца. Коммутаторы. Сети.
14. Desktop PC и network PC. Рабочие станции. Серверы. Кластерные системы.
15. MPP. SMP. NUMA.
16. Базовые установки стандартов OSI/ISO. Стандарты серии IEEE 802: подуровни LLC, MAC и PHY.
17. Процедуры обнаружения и исправления искаженных битов в структуре кадра. Базовые процедуры доступа к среде в технологии MCSA/CD: захват канала, обнаружение конфликтов, разрешение конфликтов.
18. Управление потоком в режиме скользящего окна: групповое и индивидуальное квитирование.
19. Особенности построения высокопроизводительных отказоустойчивых серверов.
20. Преимущества и проблемы многопроцессорных систем.
21. Архитектура симметричных многопроцессорных систем. Шинная и коммутаторная структуры.

22. Кластерные и массивопараллельные системы. Топология, протоколы передачи информации и методы поддержки когерентности данных.
23. Вычислительные системы, объединяющие память с микропроцессором на одном кристалле.
24. Периферийные устройства, их основные характеристики.
25. Арифметические устройства. Быстрые конвейерные алгоритмы.
26. Синхронизация параллельных процессов. Общие данные и критические секции. Программные и аппаратные способы синхронизации параллельных процессов. Семафоры и очереди.

Раздел «Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей»»

1. Системы и языки программирования, их классификация по разным критериям. Способы реализации языков в вычислительных машинах (компиляторы, интерпретаторы, компиляторы интерпретирующего типа). Понятие синтаксиса и семантики. Формальное определение словаря, грамматики и языка.
2. Скалярные типы языков типа С. Простые переменные, массивы, перечислимый тип. Указатели. Отображение их на разных архитектурах вычислительных машин.
3. "Структура" языка С как пример типа, определяемого пользователем. Тип и объект. Разные способы получения объектов. Указатели на структуру. Работа с полями.
4. Процедурный механизм в алгоритмических языках. Методы реализации для языков типа С и Фортран. Способы передачи фактических параметров. Указатели на процедуру.
5. "Классы" в языках С++ и Джава. Скрытая и интерфейсная части типа. Получение экземпляров классов (объектов). Конструкторы и деструкторы. Использование классов при программировании сложных систем как дальнейшее развитие модульного программирования.
6. Наследование классов. Правила формирования нового типа. Конструкторы наследуемого и выводимого типов, их взаимодействие. Правила приведения типов по цепочке наследования. Виртуальные функции. Множественное наследование.
7. Переопределение операций в Языке С++ как средство повышения абстрактности и универсальности программ. Примеры переопределения бинарных, унарных, пре- и пост-фиксных операций. Полиморфизм. Приоритеты при обработке управляющих символов, таких как "()".
8. Ситуационный механизм как средство взаимодействия вызывающей и вызываемой процедур. "Порождение" и "перехват" исключений в С++ и Джава. Try-блок. Реализация механизма исключений на стеке.
9. Основные концепции системы Джава. Входной язык, его отличия от С++. Концепция защищенного программирования. Независимость от платформы. Общая характеристика окружения.
10. Распараллеливание программ для современных вычислительных машин. Модели и виды параллелизма. Поддержка параллельности в архитектурах вычислительных машин. Уровни параллельности: конвейерность, многопроцессорность, мультипроцессорность.
11. Глобальные (меж- и внутри-процедурные) анализ и оптимизации. Анализ потоков управления и данных. Классические прямые и обратные алгоритмы анализа и оптимизации (распространение констант, вычисление "живых" переменных).
12. Анализ потока управления. Структурированные и неструктурированные программы. Выделение структурированных компонентов. Интервальный анализ. Приведение

- структур управления к базовым. Построение потокового графа для структурированной программы.
13. Разметка графа. Понятие критического пути. Оптимизация "втягивание в альтернативу". Устранение ложных информационных зависимостей. Оптимизация дозированным добавлением операций управления. Использование алгебраических свойств операций.
 14. Методы оптимизации циклов. Вынесение инвариантов. Индуктивные переменные. Параллельность циклов в потоковой машине и многопроцессорной системе. Наложение или совмещение операций. Опережающее считывание, запаздывающая запись, базирование регистров, выходы из циклов.
 15. Анализ зависимостей в циклах. Индексный анализ как задача целочисленного программирования. Решение систем линейных диофантовых уравнений. Экономные методы решения целочисленных неравенств. Метод Фурье-Мозкина. Выявление направлений и дистанций информационных зависимостей.
 16. Оптимальное планирование потока команд. Алгоритмы компактировки кода (приоритетное планирование списков с оптимальным назначением исполнительных устройств для ациклических программ и конвейеризованных циклов).
 17. Стратегия распределения аппаратных ресурсов при компактировке кода. Оптимизация регистров на базе алгоритма раскраски графа.
 18. Понятие об архитектуре вычислительных систем. "Аппаратная" и "программная" компоненты архитектуры. Различные типы архитектур и их примеры.
 19. Основные компоненты современных операционных систем и их характеристики.
 20. Управление памятью в современных операционных системах. Проблематика отображения адресного пространства. Сегментная, страничная и сегментно-страничная организация. Фрагментация памяти (внутренняя, внешняя). Мусорщики.
 21. Управление процессами и задачами. Понятие процесса. Классификация. Методы синхронизации (семафоры, мониторы). Потоки Джава, как пример реализации мониторов в языке программирования.
 22. Управление файлами. Структура файловых систем, стратегии распределения и защиты ресурсов, управление информацией.
 23. ОС UNIX как удачный пример мобильной операционной системы. Общая философия и основные технические решения (файлы, память, процессы, командный язык).

Раздел «Системный анализ, управление и обработка информации»

1. Топологические линейные пространства. Метрические пространства. Нормированные пространства. Примеры.
2. Выпуклые множества. Выпуклые функции. Функционал Минковского.
3. Линейные функционалы. Теоремы о продолжении линейного функционала.
4. Математические методы моделирования сложных систем. Классификация методов моделирования сложных систем. Основные этапы моделирования систем. Методы и средства имитационного моделирования сложных систем.
5. Понятия о системном подходе, системном анализе. Выделение системы из среды, определение системы. Системные понятия: вход, выход, обратная связь, ограничения.
6. Методы идентификации. Формулировка проблемы и классификация методов идентификации. Теория оценок. Теория статистических решений. Байесовский подход. Принцип минимакса. Метод максимального правдоподобия.

7. Задача принятия решения при неопределенности. Виды неопределенности и методы ее устранения.
8. Задачи многокритериальной оптимизации и методы их решения. Линейная свертка критериев. Метод контрольных показателей. Метод выделения основного критерия. Метод введения метрики в пространстве целевых функций. Метод последовательных уступок. Компромиссы Парето. Множества Парето.
9. Предпочтения и функции полезности.
10. Игры в развёрнутой и нормальной форме. Равновесия Нэша в чистых и смешанных стратегиях. Условия существования равновесия Нэша.
11. Основные понятия теории управления: цели и принципы управления, динамические системы. Динамическая система как математическая модель системы управления.
12. Математическое описание объектов управления: пространство состояний, передаточные функции, структурные схемы. Классификация систем управления.
13. Понятия управляемости и наблюдаемости систем управления.
14. Передаточная функция линейного звена. Весовая функция, переходная функция. Частотные характеристики типовых звеньев.
15. Понятие устойчивости. Устойчивость линейных стационарных систем. Критерий Михайлова. Критерий устойчивости Найквиста.
16. Фильтрация по Винеру-Хопфу. Оптимальные фильтры Калмана-Бьюси.
17. Задача на условный экстремум. Теорема Куна-Таккера и ее приложения.
18. Задача линейного программирования. Симплекс-метод. Метод эллипсоидов.
19. Сложность алгоритмов. Машина Тьюринга. Классы P и NP. NP-полные и NP-трудные задачи.
20. Метод ветвей и границ
21. Постановка задачи оптимального управления. Принцип максимума Понтрягина и его связь с вариационным исчислением.
22. Динамическое программирование, уравнение Беллмана. Достаточное условие оптимальности для задачи оптимального управления.
23. Основные понятия теории массового обслуживания (ТМО): входящие потоки требований, очереди, приборы, дисциплины обслуживания. Символика Кендалла.
24. Распределение времени ожидания начала обслуживания в ТМО. Формулы Литтля.
25. Марковские процессы. Система дифференциальных уравнений для вероятностей состояний. Достаточные условия существования стационарного режима. Система алгебраических уравнений для определения стационарных вероятностей.
26. Методы расчета критического пути в календарно-сетевом планировании. Задачи определения продолжительности проекта. Основные этапы метода PERT (Program Evaluation and Review Technique).
27. Алгоритм диспетчеризации (list scheduling) для задачи календарно- сетевого планирования в условиях ограниченных ресурсов
28. Понятие информации и информационной энтропии. Дискретный канал связи и его пропускная способность. Теорема Котельникова-Шеннона
29. Преобразования Лапласа и Лапласа-Стилтьеса, производящие функции. Вероятностная трактовка преобразования Лапласа-Стилтьеса и производящей функции.

30. Преобразование Фурье, обобщенные функции.
31. Оценки, статистические решения, проверка гипотез. Оценки параметров статистических объектов, линейная регрессия. Метод наименьших квадратов. Алгоритм LASSO, гребневая (ridge) регрессия.
32. Обучение без учителя. Задачи и алгоритмы кластеризации. Алгоритм k-средних. Иерархическая кластеризация. EM-алгоритм.
33. Методы классификации. «Наивный» байесовский классификатор, метод ближайших соседей, метод опорных векторов, деревья принятия решений.
34. Искусственные нейронные сети. Принципы и алгоритмы обучения ИНС. Алгоритм обратного распространения ошибки.

Раздел «Управление в организационных системах»

1. Предмет теории управления. Управленческие отношения и понятие организационного управления. Критерии эффективности и ограничения при достижении цели. Понятие обратной связи и ее роль в управлении. Формализация и постановка задач управления. Задачи анализа и синтеза механизмов функционирования и управления социально-экономическими системами. Основные структуры и методы управления социально-экономическими системами: административно-организационные, экономические, социально-психологические и др.
2. Основные понятия системного подхода: система, элемент, структура, среда. Свойства системы: целостность и членимость, связность, структура, организация и самоорганизация, интегрированные качества. Организация как система.
3. Понятие функций управления и их классификация, общие и специфические функции, стратегическое планирование в организационных системах управления, тактическое и оперативное планирование, оперативное управление, организация и информационное взаимодействие, модели и методы принятия решений.
4. Принципы и критерии формирования структур управления в социально-экономических системах. Основные типы организационных структур (линейные, функциональные, комбинированные, матричные), их эволюция и развитие. Особенности формирования программно-целевых структур управления на различных уровнях иерархии.
5. Методы исследования операций. Теория массового обслуживания. Управление запасами.
6. Постановка задач математического программирования. Оптимизационный подход к проблемам управления социально-экономическими системами. Допустимое множество и целевая функция. Классификация задач математического программирования. Задача линейного программирования. Теория двойственности. Симплекс-метод. Нелинейные задачи математического программирования. Локальный и глобальный экстремум, условия оптимальности, условия Куна-Таккера. Задачи об условном экстремуме и метод множителей Лагранжа. Задача стохастического программирования. Задача дискретного программирования. Метод ветвей и границ.
7. Основы теории графов: определение графа, цепи, циклы, пути, контуры. Кратчайшие пути и контуры. Поток максимальной величины. Транспортная задача. Задача о назначениях. Задачи распределения ресурса на сетях и графах. Метод динамического программирования для многошаговых задач принятия решений. Принцип оптимальности Беллмана.
8. Предмет и основные понятия теории игр. Применение теории игр для оптимизации управленческих решений. Понятие стратегии и решения игры. Равновесия: в

- доминантных стратегиях, максиминное, Нэша, Байеса, Штакельберга. Матричные игры. Игры с непротиворечивыми интересами. Кооперативные игры.
9. Методы многокритериальной оценки альтернатив. Множества компромиссов и согласия.
 10. Принятие решений в условиях неопределенности. Виды неопределенности. Статистические модели принятия решений. Критерии Байеса-Лапласа, Гермейера, Бернулли-Лапласа, максиминный (Вальда), минимаксного риска Сэвиджа, Гурвица и др.
 11. Принятие коллективных решений. Теорема Эрроу и ее анализ. Правила большинства, Кондорсе, Борда. Парадокс Кондорсе. Современные концепции группового выбора.
 12. Модели и методы принятия решений при нечеткой информации. Нечеткие множества. Основные определения и операции над нечеткими множествами. Нечеткие отношения, операции над отношениями, свойства отношений. Принятие решений при нечетком отношении предпочтений на множестве альтернатив.
 13. Социально-экономическое прогнозирование. Временные ряды и их анализ.
 14. Основы теории активных систем. Механизмы планирования в активных системах. Механизмы стимулирования в детерминированных активных системах и активных системах с неопределенностью. Базовые механизмы распределения ресурсов, активной экспертизы, конкурсные, многоканальные, противозатратные.
 15. Цели, задачи и этапы управления проектами. Методы сетевого планирования и управления. Механизмы управления проектами.
 16. Задачи и методы финансового анализа. Математические основы финансового анализа в условиях риска и неопределенности. Задача об оптимальном портфеле ценных бумаг.

Раздел «Методы и системы защиты информации, информационная безопасность»

1. Архитектура информационной безопасности. Последствия реализации угроз информационной безопасности. Источники угроз информационной безопасности.
2. Цели, задачи, способы и средства обеспечения информационной безопасности. Доступность. Конфиденциальность. Идентифицируемость. Целостность. Гарантированность.
3. Понятие целостности. Модель обеспечения целостности. Основные способы обеспечения целостности. Информация, необходимая для обеспечения целостности.
4. Формальные модели. Основные технические модели обеспечения безопасности информационных систем. Политика безопасности и формы её представления. Атрибутная модель.
5. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем.
6. Понятие доступа. Модель управление доступом (УД). Основные функции системы УД. Схемы УД (списки доступа, мандатная схема, метки доступа, контекстно-зависимая схема). Информация, необходимая для УД.
7. Криптография и криптоанализ. Ключи шифрования. Допущения при криптоанализе. Криптостойкость системы защиты информации.
8. Проблемы распространения ключей. Односторонние функции.
9. Криптосистема RSA.
10. Криптосистема Диффи-Хеллмана.

11. Каноническое разложение натуральных чисел. Алгоритмы Эвклида. Решето Эратосфена.
12. Сравнения по модулю. Малая теорема Ферма. Функция Эйлера. Китайская теорема об остатках.
13. Сложность алгоритмов сложения, умножения, возведения в целую степень.
14. Криптографические протоколы и основные требования к ним. Протоколы разделения секретов. Протоколы с нулевым разглашением.
15. Понятие идентификации и аутентификации. Способы и схемы аутентификации. Информация, необходимая для аутентификации. Проблемы защищённости способов аутентификации.
16. Классификация угроз безопасности. Типовая архитектура подсистемы защиты ОС. Разграничение доступа: основные понятия.
17. Статический метод изучения программ. Восстановление алгоритмов и структур данных.
18. Динамический метод изучения программ. Основные принципы функционирования отладчика. Метод маяков и метод трассировки. Особенности анализа параллельного кода. Поиск и определение алгоритмов шифрования.
19. Защита от дизассемблирования и отладки. Встраивание защитных средств в программное обеспечение.
20. Идентификация и аутентификация в программах. Хранение образов паролей. Атаки на системы аутентификации по паролю. Методы защиты.
21. Основные методы технической защиты от несанкционированного копирования программ и данных. Идентификация параметров компьютера. Электронные ключи.
22. Понятие компьютерного вируса. Жизненный цикл компьютерных вирусов. Разновидности компьютерных вирусов: файловые, загрузочные, макровирусы.
23. Обнаружение программных закладок. Демаскирующие признаки программных закладок. Противодействие программным закладкам: межсетевые экраны, средства обнаружения вторжений, антивирусные средства, системы контроля целостности.
24. Классификация угроз безопасности операционной системе.
25. Определение, структура и функционирование межсетевых экранов. От чего могут и не могут защитить межсетевые экраны? Понятие «демилитаризованной зоны».
26. Структура, топология и архитектура компьютерных сетей. Эталонная модель взаимодействия открытых систем. Интернет-архитектура. Архитектура ЛВС. Маршрутизация и управление потоками в компьютерных сетях.
27. Протоколы транспортного уровня и прикладного уровня Интернет-архитектуры.
28. Статическая и динамическая маршрутизация. Примеры протоколов динамической маршрутизации. Автономная система. Маршруты по умолчанию.
29. Несанкционированный обмен данными. Способы обхода межсетевых экранов. Атаки. Точка отказа всей системы. «Социальная инженерия».
30. Понятие и цель обеспечения криптоключами. Модель обеспечения криптоключами. Понятие жизненного цикла криптоключа. Модели распределения ключей. Защита криптоключей. Сертификация. Удостоверяющий центр и его основные функции.
31. Понятие безопасности баз данных. Угрозы безопасности БД: общие и специфичные. Интерпретация аспектов безопасности для БД: конфиденциальность, целостность, доступность.

32. Управление доступом к БД. Основные понятия: субъекты и объекты, группы пользователей, привилегии, роли и представления. Виды привилегий: системные и объектные. Использование ролей и привилегий пользователей.
33. Использование транзакций и блокировок для обеспечения целостности данных в БД. Фиксация и откат транзакции. Типы блокировок.
34. Атаки типа «маскарад» и их виды. Способы парирования атак типа «маскарад».
35. Понятия аудита безопасности и оповещения об опасности. Модель системы аудита безопасности. Сигналы и система оповещения об опасности. Системы обнаружения вторжений.

Литература

Вычислительные системы и их элементы

1. В.Ф.Мелехин, Е.Г.Павловский. Вычислительные машины, системы и сети. М.Издательский центр «Academia», 2010.
2. А. Танненбаум. Архитектура компьютера. СПб, Питер, 2003.
3. В. Шнитман. Современные высокопроизводительные компьютеры. М., Мир, 2003.
4. Кармахер и др. Организация ЭВМ., СПб, Питер, 2003.
5. Новиков Ю.Б., Скоробогатов П.К. Основы микропроцессорной техники. Москва, Мир, 2003
В.Г.Олифер, Н.А.Олифер. Компьютерные сети. Принципы, технологии, протоколы. 4-е издание. СПб, Питер, 2010.

Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей

1. Б. Керниган, Д.Ритчи. Язык программирования Си. Санкт-Петербург, 2003.
2. Б. Страуструп. Язык программирования C++. 4-е издание, Addison-Wesley Professional, 2013.
3. Робачевский А. М., Немнюгин С. А., Стесик О. Л. Операционная система UNIX. — 2-е изд., перераб. и доп.— СПб.. БХВ-Петербург,2010. - 656 с : ил.
4. К. Арнольд, Дж. Гослинг. Язык программирования JAVA С-Петербург: Питер, 1997.
5. Steven S.Muchnick. Computer Design and Implementation. Morgan Kaufmann Publishers, San Fransisco, California, 1997г.
6. В.А.Евстигнеев, В.Н.Касьянов Теория графов: алгоритмы обработки деревьев. ВО «Наука», Новосибирск, 1994г.
7. Banerjee, Utpal. Loop Parallelization. Softcover, 2010

Системный анализ, управление и обработка информации

1. Антонов А.В. Системный анализ: учебник для вузов / А.В. Антонов. - М.: Высшая школа, 2004. -454 с.
2. Бесекерский В.А., Попов Е.П. Теория систем автоматического управления. СПб: Профессия, 2003. -752 с.
3. Поляк Б.Т., Хлебников М.В., Рапопорт Л.Б. Математическая теория автоматического управления. М.: ЛЕНАНД, 2019.

4. Теория управления (дополнительные главы): Учебное пособие / Под ред. Д.А. Новикова, М.: ЛЕНАНД, 2019.
5. Гнеденко Б.В., Коваленко И.Н. Введение в теорию массового обслуживания. М.: Наука, 1-е издание 1968 (1980, 2005).
6. Вишнеvский В.М. Теоретические основы проектирования компьютерных сетей. – М.: Техносфера, 2003.
7. Лазарев А.А., Гафаров Е.Р. Теория расписаний: задачи и алгоритмы. М: МГУ, 2011.
8. Колмогоров А.Н., Фомин С.В. Элементы теории функций и функционального анализа. М.: Наука, 2004.
9. Поляк Б.Т. Введение в оптимизацию. М.: Ленанд. 2014.

Управление в организационных системах

1. Архипова Н.И., Кульба В.В., Косяченко С.А., Чанхиева Ф.Ю. Организационное управление : учеб. пособие для вузов. М : РГГУ, 2007. - 732 с.
2. Архипова Н.И., Кульба В.В., Косяченко С.А., Чанхиева Ф.Ю. Исследование систем управления. М.: “Издательство ПРИОР”, 2002.
3. Бурков В.Н., Заложнев А.Ю., Новиков Д.А. Теория графов в управлении организационными системами. М.: Синтег, 2001. – 124 с.
4. Бурков В.Н., Новиков Д.А. Как управлять проектами. М.: Синтег, 1997.
5. Губко М.В., Новиков Д.А. Теория игр в управлении организационными системами. М.: Синтег, 2002. – 148 с.
6. Мильнер Б.З. Теория организации. М.: ИНФРА-М, 2002. – 480 с.
7. Новиков Д.А., Петраков С.Н. Курс теории активных систем. М.: СИНТЕГ, 1999. – 108 с.

Методы и системы защиты информации, информационная безопасность

1. Компьютерные сети. 5-е издание. Э. Таненбаум, Д. Уэзеролл, М.: Мир, 2012.
2. Защита информации в компьютерных системах и сетях., Шаньгин В.Ф. М.: ДМК Пресс, 2012
3. А. Гордеев. Операционные системы — СПб.: Питер, 2007. ISBN 978-5-94723-632-3 (учебник для ВУЗов)
4. П.Ю. Белкин, О.О. Михальский, А.С. Першаков, Д.И. Правиков, В.Г. Проскурин, Г.В. Фоменков, А.Ю. Щербаков. Защита программ и данных. М.: «Радио и связь». 2003. 168 с.
5. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии: Учебное пособие. – М.: Гелиос АРВ, 2005.
6. Н. Смарт Криптография – М.: Техносфера, 2005,– 528с.
7. Черемушкин А.В. Криптографические протоколы. Основные свойства и уязвимости. Учебное пособие. Допущено УМО. М.: Изд. Центр «Академия», 2009. – 272 с.
8. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учебное пособие для вузов. М.: Горячая линия - Телеком, 2011. 320 с.
9. Мельников Д.Ю. Информационная безопасность открытых систем. Учебное пособие для вузов. – М.: ФЛИНТА, Наука, 2014. – 448 с
10. К. Дж. Дейт Введение в системы баз данных = Introduction to Database Systems. — 8-е изд. — М.: «Вильямс», 2006. — С. 1328. — ISBN 0-321-19784-4

11. Тихонов В., Райх В. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты. – М.: Гелиос АРВ, 2006 г. – 528 с.
12. В. А. Орлов, Н. В. Медведев, Н. А. Шимко, А. Б. Домрачева. Теория чисел в криптографии: Учебное пособие. – М.: МГТУ им. Н. Э. Баумана, 2011 – 223 с.
13. Стрельцов А.А. Обеспечение информационной безопасности Российской Федерации. Теоретические и методологические основы. -М, МЦНМО, 2002. -296 с.
14. ГОСТ 50922-96 «Защита информации. Основные термины и определения».
15. ГОСТ Р 51275-99 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения».