

Название вступительного испытания
Программная инженерия
Направление (-ия) подготовки
09.04.04 Программная инженерия
Образовательная программа (-мы)
09.04.04_01 Технология разработки и сопровождения качественного программного продукта 09.04.04_02 Основы анализа и разработки приложений с большими объемами распределенных данных 09.04.04_04 ИТ-инфраструктура предприятия 09.04.04_05 Управление поддержкой информационных систем, качеством и непрерывностью ИТ-сервисов
Аннотация
<p>Программа содержит перечень тем (вопросов) по дисциплинам базовой части профессионального цикла учебного плана подготовки бакалавров по направлению 09.03.04 "Программная инженерия", вошедших в содержание билетов (тестовых заданий) вступительных испытаний в магистратуру.</p> <p>Вступительное испытание оценивается по стобалльной шкале и состоит из междисциплинарного экзамена в объеме требований, предъявляемых государственными образовательными стандартами высшего образования к уровню подготовки бакалавров по направлению, соответствующему направлению магистратуры, проводимого очно в письменной форме или дистанционно (максимальный балл – 100). Минимальное количество баллов, подтверждающее его успешное прохождение устанавливается Правилами приема, утвержденными на текущий учебный год.</p> <p>Продолжительность испытания – 120 минут.</p> <p>На вступительном испытании разрешено использовать письменные принадлежности, черновик, калькулятор.</p>
Дисциплины, включенные в программу вступительных испытаний в магистратуру
<ol style="list-style-type: none"> 1. Технологии разработки качественного программного обеспечения. 2. Сети и телекоммуникации. 3. Защита информации.
Содержание учебных дисциплин
<ol style="list-style-type: none"> 1. Технологии разработки качественного программного обеспечения <ol style="list-style-type: none"> 1. Проблемы разработки программного обеспечения (ПО), модели жизненного цикла программного обеспечения (ЖЦ ПО). <ol style="list-style-type: none"> а) современные модели ЖЦ: водопадная, V-типа, спиральная, инкрементальная, итерационная, прототипная, Agile разработка ПО. б) сложность как основная проблема ПО и источники сложности. Средства борьбы со сложностью: абстракция, свертка, прогнозирование-контроль. Модульность как средство борьбы со сложностью программного проекта, прочность и сцепление модулей, интерфейс, контекст, пакетирование модулей. в) сборочная технология ПО: проблемы повторного использования модулей (reuse), возвратной инженерии (reengineering), портирования (переноса) ПО или его компонент (porting). 2. Процесс производства ПО: методы, технологии, инструментальные средства. <ol style="list-style-type: none"> а) создание проектного плана; методы оценки ресурсов и распределения работ; риск-анализ; отслеживание и контроль плана; методы и инструменты, применяемые для планирования программного проекта. б) сбор и анализ требований: источники требований, методы сбора и анализа требований; спецификация требований и согласование её с заказчиком и заинтересованными лицами проекта; язык спецификаций, формальные нотации для описания поведения системы (UML, MSC, UCM); системные требования и ПО требования; изменение, отслеживание и контроль спецификации требований. в) проектирование ПО: концептуальное (High Level Design) и детальное проектирование (Detailed Design); требования и критерии; отслеживание и контроль спецификаций архитектуры и дизайна, инструменты, применяемые при описании и исполнении дизайна. г) обзор этапа реализации проекта (кодирования); отладка, модульное тестирование (метод «белого ящика») и обзоры кода как обязательные составляющие этапа разработки ПО; стандарты кодирования. д) тестирование ПО: методы тестирования, ограничения тестирования как метода проверки ПО; инструментальные средства для тестирования и отладки многомодульных программных комплексов; макетирование ПО и внешнего окружения; интеграционное и системное тестирование; регрессионное тестирование; виды тестирования, объект тестирования в каждом из видов тестирования (функциональное тестирование, тестирование пользовательского интерфейса, тестирование безопасности, тестирование производительности ПО, тестирование удобства пользования, тестирование совместимости и др); автоматизация тестирования; способы создания тест кейсов (ручной, генерация тест кейсов по формально описанным требованиям к ПО); виды документации в тестировании; критерии тестирования ПО (стохастические критерии, мутационный критерий, структурные критерии). е) нагрузочное тестирование и тестирование производительности: этапы при проведении каждого из видов тестирования; особенности выбора инструментов для каждого вида тестирования; типы тестирования производительности (нагрузочное, тестирование стабильности, масштабируемости, отказоустойчивости, стресс тестирование, объёмное тестирование, тестирование восстановления), их цели и задачи. ж) документирование ПО: требования к ПО как промышленному продукту; стандарты на оформление

программного продукта (IEEE, ISO/МЭК, ЕСПД); виды программной документации; средства автоматизации разработки программной документации в индустриальной технологии программирования.

з) сопровождение ПО: сопровождение или продолжающаяся разработка ПО; проблемы и перспективы сопровождения ПО; используемые инструментальные средства; стиль программирования, ориентированный на поддержку этапа сопровождения.

3. Виртуализация, виды виртуализации, цели и примеры применения виртуализации (различия аппаратной виртуализации и контейнеризации). Docker инструмент для контейнеризации, использование в автоматизации тестирования ПО.

4. Веб-тестирование: жизненный цикл разработки веб-приложения, задачи тестирования веб-приложений; инструменты для автоматизации тестирования пользовательского интерфейса; инструменты для тестирования серверного компонента.

5. Метрики и управление разработкой и качеством ПО.

а) основные понятия качества и метрической теории ПО; методы оценки качества ПО (анкеты, рабочие списки, контрольные задачи, распространенные бенчмарки для оценки производительности программного изделия); методы управления качеством ПО, используемые в современных ТП (контроль и отслеживание, обзоры (review) и аудиты); аттестация ПО.

б) количественная оценка объектов с расплывчатыми свойствами: метрики и индикаторы; использование информационных и топологических метрик для оценки сложности программного модуля; конструктивные критерии качества ПО; основные модели программного модуля, используемые для оценки трудоемкости его разработки; метрики для оценки информационной сложности модулей и их использование для совокупной оценки программного проекта.

6. Современные индустриальные технологии программирования (ТП).

а) сборочная ТП, особенности ЖЦ сборочной ТП, требования к модулям и интерфейсам; быстрое программирование (agile programming), особенности ЖЦ; аспектное программирование, особенности ЖЦ, требования к модулям и интерфейсам.

б) особенности ТП: особенности ТП управляющих систем, ТП отказоустойчивых систем, ТП распределенных систем и сетей.

в) перспективные направления в развитии ТП: доказательное программирование и визуальное программирование. Метатехнология в программировании больших программных комплексов.

Литература для подготовки:

Лавров С.С. Программирование математические основы, средства, теория. - СПб. ВHV.2001. 320с.

Гленфорд Майерс, Том Баджетт, Кори Сандлер. Искусство тестирования программ, 3-е изд. – Компьютерное издательство Диалектика, 2019. – 272 с.

Котляров В.П. Основы тестирования программного обеспечения. - Национальный Открытый Университет "ИНТУИТ", 2016. -248с.

Котляров В.П., Коликова Т.В. Основы современного тестирования ПО. – М: Интернет Университет Информационных Технологий, 2006. -285с.

Непейвода Н.Н. Стили и методы программирования. - М: Интернет Университет Информационных Технологий, 2005. -320с

Мейер Б. Agile! Прекрасный, ужасный, шумный. – Москва-Тверь. НОУ «ИНТУИТ» - ЗАО НИИ ЦПС. 2015 - 248 с.

Канер С., Фолк Дж., Нгуен Енг. Тестирование программного обеспечения. –К: ДиаСофт, 2000 – 544с

Святослав Куликов. Тестирование программного обеспечения. Базовый курс, 2-е изд. EPAM Systems 2015 - 2018, версия книги 2.1.0 от 16.11.2018.

Грейди Буч, Джеймс Рамбо, Айвар Джекобсон. UML Руководство пользователя. – М.:2000 – 427с

Зыков С.В. Введение в теорию программирования,

– М: Интернет Университет Информационных Технологий, 2004. -400с

Б.Маклафлин, Г.Поллайс, Д.Уэст. Объектно-ориентированный анализ и проектирование. Питер. 2013 – 599 с.

Бозм Б. Инженерное проектирование программного обеспечения. -М: Рад. и связь, 1985. - 510с.

Оценка и аттестация зрелости процессов создания и сопровождения программных средств и информационных систем/Пер. с англ. А.С.Агапова и др. – М. Книга и бизнес. 2001. –348с.

Брукс Ф. Мифический человеко-месяц или как создаются программные системы. – Издательство Символ-Плюс (ISBN 5-93286-005-7), 2005 – 304с.

Docker Управление вычислениями (второй стен) - <https://stepik.org/course/1612/syllabus>

International Software Testing Qualifications Board Glossary. [<http://www.istqb.org/downloads/glossary.html>]

[ГОСТ 12207, 2010] – Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств. ГОСТ Р ИСО/МЭК 12207-2010, Национальный стандарт Российской Федерации, 2010.

ISO Online Browsing Platform (OBP). [<https://www.iso.org/obp/ui>]

2. Сети и телекоммуникации

1. Основы телекоммуникаций

Эволюция телекоммуникационных сетей. Общие принципы построения сетей. Коммутация каналов и

пакетов. Архитектура и стандартизация сетей. Сетевые характеристики. Эталонная модель взаимодействия открытых систем. Задачи физического уровня, уровня передачи данных, сетевого, транспортного, сеансового, представления и прикладного уровней.

2. Линии связи

Согласование характеристик каналов связи и сигналов. Линии связи и каналы передачи данных.

Характеристика проводных линий связи, волоконно-оптических линий связи и радиоканалов. Системы мобильной связи. Модели линий связи.

3. Технология физического уровня передачи данных

Методы модуляции сигналов. Коды передачи цифровых систем. Алгоритмы приема сигналов.

Помехоустойчивость приема сигналов. Методы доступа к среде передачи. Множественный доступ с частотным разделением (FDMA). Множественный доступ с временным разделением (TDMA).

Множественный доступ с кодовым разделением (CDMA). Протоколы управляемого доступа в асинхронных системах. Подуровень управления линией передачи. Методы повышения достоверности при передаче данных.

4. Сетевой уровень.

Коммутация в телекоммуникационных системах. Пространственная, временная и комбинированная коммутация каналов. Виртуальные каналы. Алгоритмы выбора маршрута в сетях с коммутацией пакетов. Алгоритмы борьбы с перегрузкой. Межсетевое взаимодействие. Туннелирование и фрагментация пакетов в объединенных сетях.

5. Локальные вычислительные сети

Структурные компоненты ЛВС: физическая среда, топология, метод доступа. Сети Ethernet и TokenRing.

Множественный доступ с контролем несущей и обнаружением конфликтов. Маркерные методы доступа.

Структура кадра. Auto-Negotiation. 10-Gigabit Ethernet. Электропитание по сети Ethernet, PoE. Аппаратные средства: сетевые контроллеры, приемопередатчики, концентраторы, коммутаторы. Интеллектуальные функции коммутаторов. Протокол STP. Маршрутизаторы. Статическая и динамическая маршрутизация.

Удаленный доступ к локальной сети. LAG. Виртуальные локальные сети. VPN. VLAN. Switch Fabric.

Планирование технических средств в базовых конфигурациях ЛВС. Высокоскоростные ЛВС.

6. Сети TCP/IP

Система протоколов стека TCP/IP для управления взаимодействием процессов в сети. Основные функции сетевого, транспортного, сеансового, представительного и прикладного уровней и базовые протоколы стека TCP/IP. Адресация, фрагментация в Интернете. Технология трансляции сетевых адресов NAT. Протокол SMTP. Протоколы Telnet, SSH. Протоколы HTTP, FTP. Протокол ICMP. TRACEROUTE. PING.

7. Технологии глобальных сетей

Структура и информационные услуги территориальных сетей. Протоколы файлового обмена, электронной почты, дистанционного управления. Виды конференц-связи. Информационная система WWW. Служба DNS. Протоколы POP3 и IMAP. Поиск в Интернете. Средства создания Web приложений.

8. Перспективы развития основных сетевых методов одновременной передачи данных, голоса, видеoinформации в направлении повышения производительности, достоверности и надежности. Методы повышения сетевой безопасности.

Литература для подготовки:

Бройдо, В. Л. Вычислительные системы, сети и телекоммуникации: учеб. для вузов / В. Л. Бройдо, О. П. Ильина. – 4-е изд. – СПб. : Питер, 2011. – 560 с.

Гусева, А. И. Вычислительные системы, сети и телекоммуникации : учеб. для вузов / А. И. Гусева, В. С. Киреев. – М. : Академия, 2014. – 288 с.

Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы : учеб. для вузов / В. Г. Олифер, Н. А. Олифер. – 5-е изд. – СПб. : Питер, 2016. – 992 с.

Пескова, С. А. Сети и телекоммуникации : учеб. для вузов. / С. А. Пескова, А. В. Кузин. – 5-е изд., перераб. – М. : Академия, 2014. – 314 с.

Пятибратов, А. П. Вычислительные системы, сети и телекоммуникации : учеб. / А. П. Пятибратов, Л. П.

Гудыно, А. А. Кириченко. – М. : КНОРУС, 2017. – 372 с.

Сети и телекоммуникации : учеб. и практикум для академического бакалавриата / под ред. К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. – М. : Юрайт, 2016. – 363 с.

Таненбаум, Э. Компьютерные сети / Э. Таненбаум, Д. Уэзерол. – 5-е изд. – СПб. : Питер, 2014. – 960 с.

3. Защита информации

Безопасность информационных технологий. Основные понятия.

Информационная безопасность, безопасность информации, безопасность информационных технологий.

Конфиденциальность, целостность, доступность.

Угрозы безопасности информационных технологий (ИТ).

Модель нарушителя.

Уязвимости информационных систем и пути нанесения ущерба.

Взаимосвязь основных понятий безопасности ИТ. Управление рисками.

Меры противодействия угрозам безопасности: законодательные, морально-этические, организационные, физические, технические.

Основные принципы построения системы защиты АС.
Шифрсистемы.
Основные понятия. Классификация криптосистем.
Классификация шифрсистем. Простые шифры.
Теоретико-информационная оценка криптостойкости шифрсистем. Совершенно безопасные системы.
Ненадежность шифров и расстояние единственности.
Практическая стойкость шифра. Современные методы и технологии криптоанализа.
Требования к современным шифрам (диффузия, конфузия, практическая реализуемость). Итерированные блочные шифры. Выбор основных параметров.
Требования к шифрам первого поколения. Сеть Фейстела.
Блочный шифр ГОСТ 28147-89. Основные характеристики. Математическая модель и архитектура.
Требования к шифрам второго поколения. Блочный шифр AES. Основные характеристики. Математическая модель и архитектура.
Сравнительный анализ современных блочных шифров.
Протоколы шифрования. ГОСТ 28147-89. Режим простой замены. Математическая модель, особенности и области применения.
Протоколы шифрования. ГОСТ 28147-89. Режим гаммирования. Математическая модель, особенности и области применения.
Протоколы шифрования. ГОСТ 28147-89. Режим гаммирования с обратной связью. Математическая модель, особенности и области применения.
Сравнительный анализ протоколов шифрования ГОСТ 28147-89 и стандартов США.
Обеспечение имитостойкости.
Имитостойкость.
Способы контроля целостности сообщения.
Хэш-функция. Требования к криптографической хэш-функции. Криптостойкость хэш-функций.
Архитектура хэш-функции. Функция сжатия.
Стандарт функции хэширования ГОСТ Р34.11-94. Основные характеристики и математическая модель.
Сравнительные характеристики современных хэш-функций.
Стандарт функции хэширования SHA-1. Основные характеристики и математическая модель.
Сравнительные характеристики современных хэш-функций.
Протокол контроля целостности с использованием хэш-функции. Область применения.
Коды аутентификации сообщения. Математическая модель. Достоинства и недостатки. Область применения.
HMAC. Математическая модель и основные характеристики. Протокол контроля целостности. Область применения.
Шифрование с контролем целостности. Показатели эффективности. Стандарт блочного шифрования ГОСТ 28147-89, режим выработки имитовставки. Математическая модель и основные характеристики. Протокол контроля целостности.
Сравнительный анализ протоколов контроля целостности.
Методы защиты от навязывания ранее переданных, задержанных или переадресованных сообщений.
Криптография с открытым ключом
Требования к преобразованиям в криптографии с открытым ключом. Вычислительно простые и вычислительно сложные проблемы.
Необратимые преобразования с лазейкой и их применение в криптографии с открытым ключом..
Система открытого шифрования RSA. Математическая модель. Протокол применения. Анализ криптостойкости.
Сравнительный анализ шифрования с секретным ключом и открытого шифрования.
Электронная цифровая подпись (ЭЦП).
Модель нарушителя и требования к ЭЦП. Сравнение с графической подписью.
ЭЦП RSA, математическая модель, анализ криптостойкости, протокол применения. ЭЦП ElGamal, математическая модель, анализ криптостойкости. Сравнение ЭЦП ElGamal и ЭЦП RSA. ЭЦП DSA, математическая модель, анализ криптостойкости. Математические основы криптографии на эллиптических кривых (ЭК).
ЭЦП на ЭК (ГОСТ Р34.10-2001), математическая модель, анализ криптостойкости, протокол применения.
Сравнительные характеристики ЭЦП (RSA, DSA, ГОСТ Р34.10-2001 (ECDSA)).
Хэш-функции в протоколах цифровой подписи.
Управление криптографическими ключами.
Жизненный цикл ключей и функции управления ключами.
Криптографические генераторы псевдослучайных последовательностей (требования, принципы построения, примеры).
Генерация больших простых чисел. Тест Ферма.
Управление ключами в криптосистемах с секретным ключом, сравнительный анализ протоколов децентрализованного и централизованного управления ключами.
Управление ключами в криптосистемах с открытым ключом. Сертификат открытого ключа. Удостоверяющий центр и его функции. Протоколы сертификации и кросс-сертификации.
Гибридные криптосистемы на основе открытого шифрования и открытого распределения ключей системы.

Аутентификация субъектов.

Идентификация и аутентификация. Классификация схем аутентификации. Требования к протоколу аутентификации.

Парольная защита. Достоинства и недостатки (уязвимости). Методы усиления парольной защиты.

Аутентификация с использованием криптографических методов. Примеры протоколов.

Аутентификация с нулевой передачей знаний. Протокол Fiat-Shmir, математическая модель, протокол применения, анализ стойкости.

Биометрическая аутентификация. Статические и динамические биометрические образы. Биометрические механизмы. Биометрическая аутентификация и криптографические механизмы.

Разграничение доступа.

Политика безопасности и схема разграничения доступа. Избирательное управление доступом.

Математическая модель. Достоинства и недостатки.

Полномочное управление доступом. Математическая модель. Особенности применения и реализации.

Ролевая модель управления доступом. Математическая модель. Достоинства и недостатки.

Контроль информационных потоков для обеспечения конфиденциальности (модель Bell-LaPadule).

Достоинства и недостатки.

Реализация разграничения доступа в современных ОС.

Безопасность компьютерных сетей.

Уязвимости IP-сетей, сетевых ОС и прикладных сервисов. Типовые сетевые атаки. Защищенный сетевой протокол IPSec, Архитектура: протоколы безопасности (TSP, AH) и режимы их использования, ассоциация безопасности и протокол согласования ее параметров (ISAKMP), БД политик безопасности.

Защищенный транспортный протокол SSL, архитектура и принципы работы. Межсетевые экраны (МЭ).

Основные функции. Типы МЭ. Построение и применение правил фильтрации. Конфигурация МЭ.

Оценочные стандарты безопасности информационных технологий.

Нормативные стандарты. «Оранжевая книга» Концепция, основные понятия. Достоинства и недостатки.

Руководящие документы Гостехкомиссии: «Показатели защищенности от НСД к информации»,

«Классификация АС и требования по защите информации». Концепция, основные понятия, принципы применения, достоинства и недостатки.

ГОСТ ISO/IEC 15408 «Общий критерий оценки безопасности информационных технологий». Концепция

документа. Основные понятия: требования безопасности (функциональные и доверия) и их структуризация, уровни доверия, профиль защиты). Принципы применения.

Литература для подготовки:

Габидулин Э. М., Кшевецкий А. С., Колыбельников А. И. Защита информации: учебное пособие — М.: МФТИ, 2011. — 225 с. http://permsite.ru/files/2017/12/information_security_Z3WChDA.pdf

Партыка, Т. Л. Информационная безопасность : учеб. пособие для вузов / Т. Л. Партыка, И. И. Попов. – 5-е изд., перераб. и доп. – М. : ФОРУМ : ИНФА-М, 2014. – 432 с.

Хорев, П. Б. Программно-аппаратная защита информации : учеб. пособие для вузов / П. Б. Хорев. – 2-е изд., испр. и доп. – М. : ФОРУМ : ИНФА-М, 2015. – 352 с.

Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учеб. пособие для вузов / В. Ф. Шаньгин. – М. : ИД ФОРУМ : ИНФА-М, 2014. – 416 с.

Критерии оценивания вступительного испытания

Междисциплинарный экзамен состоит из 50 тестовых заданий. Максимальный балл за задание - 2.

Рабочая группа

Руководители ОП:

Профессор ВШПИ ИКНК, д.т.н. С.А. Молодяков

Доцент ВШПИ ИКНК, к.т.н. И.В. Никифоров

Старший преподаватель ВШПИ ИКНК Е.А. Павлов

Составители:

Профессор ВШПИ ИКНК, д.т.н. С.А. Молодяков

Доцент ВШПИ ИКНК, к.т.н. В.В. Амосов

Ст. преподаватель ВШПИ ИКНКЛ.П. Котлярова