МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Воронежский государственный технический университет»

УТВЕРЖДАЮ
Декан факультета _____ С.М. Пасмурнов
«31» августа 2017 г.

РАБОЧАЯ ПРОГРАММА

дисциплины

«Информационная безопасности распределённых информационных систем»

Специальность 10.05.03 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Специализация Обеспечение информационной безопасности распределенных информационных систем

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет

Форма обучения очная

Год начала подготовки 2017

Автор программы _____ /Язов Ю.К./

Заведующий кафедрой
Систем информационной
безопасности _____ / А.Г. Остапенко /

Руководитель ОПОП _____ / А.Г. Остапенко /

Воронеж 2017

1.ЦЕЛИИЗАДАЧИДИСЦИПЛИНЫ

1.1.Цельдисциплиныпредоставить студентам возможность освоения подходов к анализу и синтезу проектных решений при реализации распределённых информационных систем, а также обучить их основам выявления и противодействия атакам вредоносных программ и злоумышленников в распределенных системах обработки информации.

1.2.Задачиосвоениядисциплины

- формирование системных представлений об анализе и синтезе структуры, состава систем защиты распределенной информационной системы;
- изучение методологии обнаружения уязвимостей распределенной информационной системы;
- изучение методологии контроля эффективности системы безопасности распределенной информационной системы.

2.МЕСТОДИСЦИПЛИНЫВСТРУКТУРЕОПОП

Дисциплина«Информационнаябезопасностираспределённыхинформационныхсистем»относитсякдисциплинамбазовойчастиблокаБ1.

3.ПЕРЕЧЕНЬПЛАНИРУЕМЫХРЕЗУЛЬТАТОВОБУЧЕНИЯПОДИСЦИПЛИНЕ

Процессизучениядисциплины«Информационнаябезопасностираспределённыхинформационныхсистем»направленнаформированиеследующихкомпетенций:

ПК-2-способностьюсоздаватьиисследоватьмоделиавтоматизированных систем

ПК-8-способностьюразрабатыватьианализироватьпроектныерешенияпообеспечениюбезопасностиавтоматизированныхсистем

ПК-24-способностьюобеспечитьэффективноеприменениеинформационно-технологическихресурсовавтоматизированнойсистемысучетомтребований информационнойбезопасности

ПСК-7.1-способностьюразрабатыватьиисследоватьмоделиинформационно-технологическихресурсов,разрабатыватьмоделиугрозимоделинарушителяинформационнойбезопасностивраспределенныхинформационныхсистемах

ПСК-7.2-способностьюпроводитьанализрисковинформационнойбезопасностииразрабатывать,руководитьразработкойполитикибезопасностивраспределенныхинформационныхсистемах

Компетенция	**Результатыобучения,характеризующие сформированностькомпетенции**
ПК-2	знать принципы системного похода к созданию иисследованиюмоделиавтоматизированныхсистем
	уметьсоздавать и исследовать модели автоматизированных систем

	владеть инструментальными средствами создания и исследования моделей автоматизированных систем
ПК-8	знать основные методы параметрического и структурного синтеза, критериев оптимизации и методы математического программирования с целью анализа проектных решений, в том числе и решений пообеспечениюбезопасностиавтоматизированны хсистем
	уметь применять основные методы параметрического и структурного синтеза, критериев оптимизации и методы математического программирования с целью анализа проектных решений, в том числе и решений пообеспечениюбезопасностиавтоматизированны хсистем
ПК-24	знать основные методы параметрического и структурного синтеза, критериев оптимизации и методы математического программирования с целью анализа проектных решений, в том числе и решений пообеспечениюбезопасностиавтоматизированны хсистем
	уметь применять основные методы параметрического и структурного синтеза, критериев оптимизации и методы математического программирования с целью анализа проектных решений, в том числе и решений пообеспечениюбезопасностиавтоматизированны хсистем
ПСК-7.1	знатьметоды и средства обнаружения уязвимостей распределенной информационной системы, методы и средства обнаружения атак на ресурсы распределенной информационной системы, а также методы и средства противодействия атакам на ресурсы распределенной информационной системы
	уметь разрабатыватьиисследоватьмоделиинформационно-технологическихресурсов,разрабатыватьмоделиугрозимоделинарушителяинформационнойб

	езопасностиврaспределенныхинформационныхсистемах
ПСК-7.2	знатьметодику разработкиполитикибезопасностиврaспределенныхинформационныхсистемах
	уметь проводитьанализрисковинформационнойбезопасности

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общаятрудоемкостьдисциплины«Информационнаябезопасностираспределённыхинформационныхсистем»составляет6з.е.

Распределениетрудоемкостидисциплиныповидамзанятий

очнаяформаобучения

Видыучебнойработы	Всегочасов	Семестры
		7
Аудиторныезанятия (всего)	72	72
В томчисле:		
Лекции	36	36
Лабораторныеработы (ЛР)	36	36
Самостоятельнаяработа	108	108
Курсовойпроект	+	+
Часынаконтроль	36	36
Видыпромежуточнойаттестации - экзамен	+	+
Общая трудоемкость: академические часы зач.ед.	 216 6	 216 6

5.СОДЕРЖАНИЕДИСЦИПЛИНЫ(МОДУЛЯ)

5.1Содержаниеразделовдисциплиныираспределениетрудоемкостиповидамзанятий

очнаяформаобучения

№ п/п	Наименованиетемы	Содержаниераздела	Лекц	Лаб. зан.	СРС	Всего, час
1	Принципы системного похода к созданию иисследованиюмоделейавтоматизированныхсистем	Системный подход к проектированию. Понятие инженерного проектирования. Принципы системного подхода. Основные понятия системотехники. Иерархическая структура проектных спецификаций и иерархические уровни	6	6	18	30

		проектирования. Стадии проектирования. Содержание типовых ТЗ. Классификация моделей и параметров, используемых при автоматизированном проектировании информационных систем				
2	Математическое обеспечение анализа и синтеза проектных решений	Компоненты математического обеспечения. Математические модели в процедурах анализа на макроуровне. Методы и алгоритмы анализа на макроуровне Математическое обеспечение анализа на микроуровне Математическое обеспечение анализа на функционально-логическом уровне Математическое обеспечение анализа на системном уровне. Математическое обеспечение синтеза проектных решений. Постановка задач параметрического синтеза. Обзор методов оптимизации. Постановка задач структурного синтеза. Методы структурного синтеза	6	6	18	30
3	Принципы проектирования архитектуры и структуры распределенных систем обработки информации	Основные понятия. Распределенная информационная система, ее функции. Полностью неоднородные, частично однородные и однородные распределенные системы обработки данных. Классификация распределенных информационных систем по архитектурным особенностям и по степени распределённости. Способы организации взаимодействия между ЭВМ. Характеристики распределенной информационной системы. Технология «клиент-сервер». Серверы приложений и прикладные протоколы. Представление данных в информационных системах. Логическая, физическая и программная структуры распределенной информационной системы. Назначение и функции элементов этих структур. Концепция взаимодействия открытых систем. Иерархия системы обработки данных: уровень архитектуры системы обработки данных, среда для конечного пользователя и инструментарий прикладного программиста, операционная система, оборудование. Объектно-ориентированные системы.	6	6	18	30

		Свойства открытых систем и объектно-ориентированных систем программирования				
4	Атаки на интрасети и интернет-сети	Интрасети и Интернет-сети Локальные сети LAN и глобальные (региональные) сети WAN, сетевые комплексы или объединенные сети. Термины Карта Сетевого Интерфейса, Физический Порт, Интерфейсы. Стандартные обозначения компонентов сетей. Понятие «интрасеть». Различие интрасети и Интернет-сети. Возможности и предоставляемые услуги. Порядок предоставления доступа Виды доступа. Обязанности пользователей. Права и обязанности управления информатизации по администрированию интрасети. Абсолютно упругий и неупругий удар. Атаки на интрасети и Интернет-сети. Классификация типов удаленных атак на интрасети по степени риска (RiskFactor), по типу атаки (AttackType), по подверженному данной атаке программному обеспечению (PlatformsAffected). Анализ сетевого трафика. Подмена доверенного объекта. Введение ложного объекта компьютерной сети. Отказ в обслуживании (DoS). Сканирование компьютерных сетей. Сети botnet (BlueCoatSecurityLabs). Эволюция угроз. Классификация угроз безопасности Web-приложений. Аутентификация. Авторизация. Атаки на клиентов. Выполнениекода. Разглашениеинформации. Логическиеатаки.	6	6	18	30
5	Основы построения систем обнаружения вторжений	Понятие «Система обнаружения вторжений». Функции системы обнаружения вторжений. Виды систем обнаружения вторжений. Пассивные и активные системы обнаружения вторжений. Основные компоненты системы обнаружения вторжений: датчики (сенсоры) и анализаторы. Принципы функционирования систем обнаружения вторжений Структура современных систем обнаружения вторжений. Сущность и функции ее подсистем: подсистемы сбора информации, подсистемы	6	6	18	30

		анализа и подсистемы представления данных. Анализ недостатков современных систем обнаружения вторжений. Требования по безопасности информации. Функциональные требования безопасности для систем обнаружения вторжений. Механизмы защиты. Профили защиты системы обнаружения вторжений. Идентификация профиля защиты. Организация профиля защиты. Методы обнаружения вторжений Подходы к защите от типовых удаленных атак на интрасети. Методы обнаружения аномалий: моделирование правил, описательная статистика, нейронные сети, моделирование множества состояний, описательная статистика. Методы обнаружения злоупотреблений: моделирование состояний, экспертные системы, моделирование правил, синтаксический анализ. Методы, основанные на моделировании поведения злоумышленника. Технологии построения систем обнаружения атак Существующие технологии построения систем обнаружения атак. Технологии обнаружения аномальной деятельности. Статистический анализ компьютерных атак. Анализ систем, использующих сигнатурные методы. Анализ систем, использующих методы поиска аномалий в поведении. Общая оценка современного подхода к обнаружению вторжений. Концепция обнаружения компьютерных угроз				
6	Контроль эффективности системы безопасности распределенной информационной системы	Стандарты управления информационной безопасностью Стандарты ISO/IEC 17799:2002 (BS 7799:2000) – ГОСТ Р ИСО/МЭК 17799 «Управление информационной безопасностью — Информационные технологии» (Informationtechnology — Informationsecuritymanagement») Повышение эффективности систем обнаружения атак — интегральный подход. Сценарий атаки. Фазы атаки. Схема интегрального обнаружения компьютерных атак. Эффективность	6	6	18	30

		проверки правил в системах обнаружения сетевых атак. Требования доверия к безопасности системы обнаружения вторжений. Аудит безопасности. Управление безопасностью. Администрирование безопасности. Административные, технические (логические) и физические меры. Администрирование информационной системы в целом. Администрирование сервисов безопасности. Администрирование механизмов безопасности. Обязанности и ответственность администратора. Поддержка безопасности в распределенной системе Типичные проблемы безопасности.				
			Итого	**36**	**36**	**108**	**180**

5.2Перечеьлабораторныхработ

Математическое обеспечение анализа и синтеза проектных решений

Решение компонентных уравнений в GNUOctave. Решения систем линейных алгебраических уравненийв GNUOctave. Анализ в частотной областив GNUOctave.

Принципы проектирования архитектуры и структуры распределенных систем обработки информации

HTML-редактор Dreamweaver MX. Знакомство с интерфейсом программы Dreamweaver. Предварительная настройка Dreamweaver.

Dreamweaver. Набор и форматирование текста. Работа с таблицами.

Атаки на интрасети и интернет-сети

Dreamweaver. Вставка графических изображений. Создание гиперссылок. Знакомство со справочной системой.

Dreamweaver. Создание документа с фреймами

Dreamweaver. Создание документа с формами

Основы построения систем обнаружения вторжений

Использование программы Dr. WEB

Использование программы Dr. WEB в режиме графического интерфейса

Изучение JavaScript. Создание кнопки

Изучение JavaScript. Бегущая строка

Изучение JavaScript. Горизонтальное меню.

Контроль эффективности системы безопасности распределенной информационной системы

Изучение JavaScript. Показ баннера.

Настройка для MicrosoftInternetExplorer для обеспечения безопасности использования WWW.

6.ПРИМЕРНАЯТЕМАТИКАКУРСОВЫХПРОЕКТОВ(РАБОТ) ИКОНТРОЛЬНЫХРАБОТ

Всоответствиисучебнымпланомосвоениедисциплиныпредусматриваетвыполнениекурсовогопроектав7семестредляочнойформыобучения.

Примерная тематика курсового проекта: «Проектирование системы распределённой информационной системы анализа и прогнозирования потребности в трудовых ресурсах».

Задачи, решаемые при выполнении курсового проекта:

- систематизировать, закрепить и расширить теоретические знания по дисциплине;
- развить навыки ведения самостоятельной работы и овладения методикой исследовательской, проектно-аналитической деятельности и т.д.;
- освоить современные методы и средства проектирования архитектуры и структуры распределенных систем обработки информации
- развить навыки презентации результатов выполненных исследований и расчетов.

Курсовой проект включат в себя графическую часть и расчет-но-пояснительную записку

7.ОЦЕНОЧНЫЕМАТЕРИАЛЫДЛЯПРОВЕДЕНИЯПРОМЕЖУТОЧНОЙАТТЕСТАЦИИОБУЧАЮЩИХСЯПОДИСЦИПЛИНЕ

7.1.Описаниепоказателейикритериевоцениваниякомпетенцийнаразличныхэтапахихформирования,описаниешкалоценивания

7.1.1Этаптекущегоконтроля

Результатытекущегоконтролязнанийимежсессионнойаттестацииоцениваютсяпоследующейсистеме:

«аттестован»;

«неаттестован».

Компе-тенция	Результатыобучения,характеризующие сформированностькомпетенции	Критерии оценивания	Аттестован	Неаттестован
ПК-2	знать принципы системного похода к созданию иисследованиюмоделиавтоматизированныхсистем	знать принципы системного похода к созданию иисследованиюмоделиавтоматизированныхсистем	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметьсоздавать и исследовать модели автоматизированных систем	уметьсоздавать и исследовать модели автоматизированных систем	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть инструментальными средствами создания и	владеть инструментальными средствами создания и	Выполнение работ в	Невыполнение работ

	исследования моделей автоматизированных систем	исследования моделей автоматизированных систем	срок, предусмотренный в рабочих программах	в срок, предусмотренный в рабочих программах
ПК-8	знать основные методы параметрического и структурного синтеза, критериев оптимизации и методы математического программирования с целью анализа проектных решений, в том числе и решений пообеспечениюбезопасностиавтоматизированныхсистем	знать основные методы параметрического и структурного синтеза, критериев оптимизации и методы математического программирования с целью анализа проектных решений, в том числе и решений пообеспечениюбезопасностиавтоматизированныхсистем	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь применять основные методы параметрического и структурного синтеза, критериев оптимизации и методы математического программирования с целью анализа проектных решений, в том числе и решений пообеспечениюбезопасностиавтоматизированныхсистем	уметь применять основные методы параметрического и структурного синтеза, критериев оптимизации и методы математического программирования с целью анализа проектных решений, в том числе и решений пообеспечениюбезопасностиавтоматизированныхсистем	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-24	знать основные методы параметрического и структурного синтеза, критериев оптимизации и методы математического программирования с целью анализа проектных решений, в том числе и решений пообеспечениюбезопасностиавтоматизированныхсистем	знать основные методы параметрического и структурного синтеза, критериев оптимизации и методы математического программирования с целью анализа проектных решений, в том числе и решений пообеспечениюбезопасностиавтоматизированныхсистем	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь применять основные методы параметрического и структурного синтеза, критериев оптимизации и методы математического программирования с целью анализа проектных решений, в том числе и решений пообеспечениюбезопасностиавтоматизированныхсистем	уметь применять основные методы параметрического и структурного синтеза, критериев оптимизации и методы математического программирования с целью анализа проектных решений, в том числе и решений пообеспечениюбезопасностиавтоматизированныхсистем	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПСК-7.1	знать методы и средства обнаружения уязвимостей распределенной информационной системы, методы и средства обнаружения атак на ресурсы распределенной информационной системы, а также методы и	знать методы и средства обнаружения уязвимостей распределенной информационной системы, методы и средства обнаружения атак на ресурсы распределенной	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

	средства противодействия атакам на ресурсы распределенной информационной системы	информационной системы, а также методы и средства противодействия атакам на ресурсы распределенной информационной системы		
	уметь разрабатыватьиисследоватьмодели информационно-технологическихр есурсов,разрабатыватьмоделиугро зимоделинарушителяинформацио ннойбезопасностиврaспределенны хинформационныхсистемах	уметь разрабатыватьиисследоватьм оделиинформационно-технол огическихресурсов,разрабаты ватьмоделиугрозимоделинару шителяинформационнойбезо пасностиврaспределенныхин формационныхсистемах	Выполнен ие работ в срок, предусмот ренный в рабочих программ ах	Невыполн ение работ в срок, предусмот ренный в рабочих программа х
ПСК-7.2	знать методику разработкиполитикибезопасностив распределенныхинформационныхс истемах	знаниеметодики разработкиполитикибезопасн остиврaспределенныхинформ ационныхсистемах	Выполнен ие работ в срок, предусмот ренный в рабочих программ ах	Невыполн ение работ в срок, предусмот ренный в рабочих программа х
	уметь проводитьанализрисковинформац ионнойбезопасности	умение проводитьанализрисковинфор мационнойбезопасности	Выполнен ие работ в срок, предусмот ренный в рабочих программ ах	Невыполн ение работ в срок, предусмот ренный в рабочих программа х

7.1.2Этаппромежуточногоконтролязнаний

Результатыпромежуточногоконтролязнанийоцениваютсяв7семестредля очнойформыобученияпочетырехбалльнойсистеме:

«отлично»;

«хорошо»;

«удовлетворительно»;

«неудовлетворительно».

Компе-тенция	**Результатыобучения,характеризующие сформированностькомпетенции**	**Критерии оценивания**	**Отлично**	**Хорошо**	**Удовл.**	**Неудовл.**
ПК-2	знать принципы системного похода к созданию иисследованиюмоделиавтом атизированныхсистем	Тест	Выполнениетестана 90-100%	Выполнениетестана 80- 90%	Выполнениетестана 70- 80%	В тесте менее 70% правильных ответов
	уметьсоздавать и исследовать модели автоматизированных систем	Решениестандартныхпрактическихзадач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи нерешены

	владеть инструментальными средствами создания и исследования моделей автоматизированных систем	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи нерешены
ПК-8	знать основные методы параметрического и структурного синтеза, критериев оптимизации и методы математического программирования с целью анализа проектных решений, в том числе и решений пообеспечениюбезопасности автоматизированныхсистем	Тест	Выполнение тестана 90-100%	Выполнениетестана 80- 90%	Выполнениетестана 70- 80%	В тесте менее 70% правильных ответов
	уметь применять основные методы параметрического и структурного синтеза, критериев оптимизации и методы математического программирования с целью анализа проектных решений, в том числе и решений пообеспечениюбезопасности автоматизированныхсистем	Решениестандартныхпрактическихзадач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи нерешены
ПК-24	знать основные методы параметрического и структурного синтеза, критериев оптимизации и методы математического программирования с целью анализа проектных решений, в том числе и решений пообеспечениюбезопасности автоматизированныхсистем	Тест	Выполнение тестана 90-100%	Выполнениетестана 80- 90%	Выполнениетестана 70- 80%	В тесте менее 70% правильных ответов
	уметь применять основные методы параметрического и структурного синтеза, критериев оптимизации и методы математического программирования с целью анализа проектных решений, в том числе и решений пообеспечениюбезопасности автоматизированныхсистем	Решениестандартныхпрактическихзадач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи нерешены
ПСК-7.1	знать методы и средства обнаружения уязвимостей распределенной информационной системы, методы и средства обнаружения атак на	Тест	Выполнение тестана 90-100%	Выполнениетестана 80- 90%	Выполнениетестана 70- 80%	В тесте менее 70% правильных ответо

	ресурсы распределенной информационной системы, а также методы и средства противодействия атакам на ресурсы распределенной информационной системы					в
	уметь разрабатыватьиисследовать моделиинформационно-технологическихресурсов,разрабатыватьмоделиугрозимоделинарушителяинформационнойбезопасностиврасределенныхинформационныхсистемах	Решениестандартныхпрактическихзадач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи нерешены
ПСК-7.2	знать методику разработкиполитикибезопасностиврасределенныхинформационныхсистемах	Тест	Выполнениетестана 90-100%	Выполнениетестана 80- 90%	Выполниетестана 70- 80%	В тесте менее 70% правильных ответов
	уметь проводитьанализрисковинформационнойбезопасности	Решениестандартныхпрактическихзадач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи нерешены

7.2Примерныйпереченьоценочныхсредств(типовыеконтрольныезаданияилиныематериалы,необходимыедляоценкизнаний,умений,навыкови(или)опытадеятельности)

7.2.1Примерныйпереченьзаданийдляподготовкиктестированию

1. Какая модель изображена на рисунке?

+ клиент-сервер

2. Вставьте слово.
Процессы, реализующие некоторую службу, например службу файловой системы или базы данных, называются...
+ серверами

3. Вставьте слово.
Процессы, запрашивающие службы у серверов путем посылки запроса и последующего ожидания ответа от сервера, называются...
+ клиентами

4. Что дает архитектура клиент-сервер?
+ надежность
- возможность редактировать
+ масштабируемость
- доступ
+ безопасность
+ гибкость

5. Извлечение информации это - ...

- способ защиты информации

+ это задача автоматического извлечения (построения) структурированных данных из неструктурированных или слабоструктурированных машиночитаемых документов.

- преобразование информации из одного вида в другой, осуществляемое по строгим формальным правилам.

6. Вставьте слово

.... является стандартным языком, предназначенным для создания гипертекстовых документов в среде WEB.

+HTML

7. Язык разметки документов – это

- это структурная единица XML- документа.

+ набор специальных инструкций, называемых тегами, предназначенных для формирования в документах какой-либо структуры и определения отношений между различными элементами этой структуры.

- преобразование информации из одного вида в другой, осуществляемое по строгим формальным правилам.

8. Выберите чветуказанный в значении RGB - "#000000"

+ черный
- белый
- серый
- зеленый
- желтый

9. Что относится к атрибутам тэга для форматирования шрифтов < FONT>< /FONT>.

- align
+ color

+ face
- noshade
+ size

10. Вставьтетег

Для добавления изображения на веб-страницу используется тег...
+

11. Каскадные (многоуровневые) таблицы стилей - это

- мощный инструмент, который позволяет создавать образцы стилей, которые можно затем применять ко всему узлу.

+ мощный стандарт на основе текстового формата, определяющий представление данных в броузере.

-это мощный инструмент позволяющий контролировать всю страницу HTML.

12. Что входит в сферы применения Java-технологий:

+ разработка приложений (application)
+ разработка мидлетов (midlet)
+ разработка апплетов (applet)
- разработка таблиц
+ разработка JSP-страниц
+ разработка сервлетов (servlet)

13. Какие бывают ошибки в коде программ PHP?

+ ошибочная ситуация
+ внутренняя ошибка
- внешня ошибка
+ пользовательская ошибка
- ошибка работы

14. Какие стили синтаксиса регулярных выражений поддерживает PHP?

- Ereg_replace
+ POSIX
+ Perl
- Split

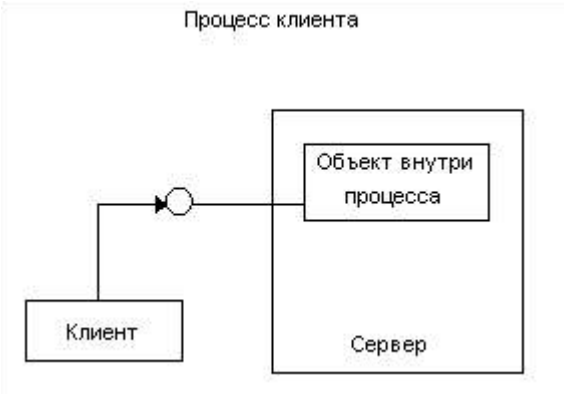
15. COM-объект

- это классы, которые содержат один или более COM-интерфейс.

+ представляет собой двоичный код, который выполняет какую-либо функцию и имеет один или более интерфейс.

- представляет собой приложение или библиотеку, которая предоставляет услуги приложению-клиенту или библиотеке.

16. На рисунке схема взаимодействия клиента с...



+ внутреннимсервером

7.2.2Примерныйпереченьзаданийдлярешениястандартныхзадач

1. Верны ли утверждения?В состав КИС бизнес-объекта (фирмы или предприятия) могут входить:А) система анализа данных OLAP;В) система представления данных для анализа руководством (MIS);

А-нет,В-Да

А-да, В-нет

А-да, В-да

А-нет, В-нет

2.Кооперация агентов - это

кооперация, которая регламентируется набором соглашений между агентами

непреднамеренное сотрудничество между агентами, направленное на выживание агентов

принудительное сотрудничество между агентами

добровольное сотрудничество между агентами

3. Верны ли утверждения?

К архитектурам МАСотносятся архитектуры:А) реактивная; Б)гибридная

А-нет,В-Да

А-да, В-нет

А-да, В-да

А-нет, В-нет

4.Оптимизационные модели СППР: А)описывают поведение некоторой системы и не предназначены для целей управления; В)служат для нахождения точек минимума или максимума некоторых показателей

А-нет,В-Да

А-да, В-нет

А-да, В-да

А-нет, В-нет

5.К количественным показателям, учитываемым при проектировании распределенной реляционном БД, относятся: А)используемые отношения, атрибуты и строки; В) частота выполнения транзакции

А-нет,В-Да

А-да, В-нет

А-да, В-да

А-нет, В-нет

6. Верны ли утверждения?

В состав КИС бизнес-объекта (фирмы или предприятия) могут входить: А)система документооборота (DocFlow); В)система организации рабочего пространства (Workflow);

А - нет, В - да

А - нет, В – нет

А - да, В – да

А - да, В – нет

7. Верны ли утверждения?

Классы сеансовых и объектных компонентов реализуют: А)прикладные методы компонента; В) интерфейс компонента

А - нет, В – да

А - да, В - да

А - нет, В – нет

А - да, В - нет

8. Устройства агента, непосредственно воспринимающие воздействия внешней среды, - это

рецепторы

эффекторы

процессоры

блоки памяти

9. Характеристиками взаимодействия агентов являются:

А) избирательность:

В) реактивность

А-да,В-нет

А-нет,В-нет

А - нет, В - да

А - да, В - нет

10. OLAP-системы должны автоматически настраивать свою физическую схему в зависимости от типа модели, объемов данных и разреженности базы данных - это по Кодду для OLAP-систем

динамическое управление разреженными матрицами

интуитивная манипуляция данными

неограниченная размерность и число уровней агрегации

прозрачность

7.2.3Примерныйпереченьзаданийдлярешенияприкладныхзадач

1. В задаче линейного программирования введением дополнительных переменных можно

1) преобразовать линейную форму к нелинейной

2) свести ограничения типа равенств к неравенствам

3) свести ограничения типа неравенств к равенствам

4) уменьшить число ограничений

2. Каноническая фора задачи при решении ее симплекс-методом должна содержать:

1) только отрицательные переменные и ограничения типа неравенств

2) только отрицательные переменные и ограничения типа равенств

3) только положительные переменные и ограничения типа неравенств

4) только положительные переменные и ограничения типа равенств

3.Метод поиска экстремума путем последовательного деления отрезка пополам называется

1) методом дихотомии

2) поиском однородными парами

3) пассивным поиском

4) параллельным поиском

4. Точки, в которых первые производные функции обращаются в ноль, называются

1) стационарными

2) оптимальным

3) экстремальными

4) перегиба

5. Задачи целочисленного программирования решаются

1) методом Ньютона

2) методом дихотомии

3) методом Гомори

4) методом искусственного базиса

6. Базисная переменная это…

1) переменная, на которую не наложено условие неотрицательности

2) переменная, на которую наложено условие целочисленности

3) переменная, которая входит только в одно ограничение с единичным коэффициентом

7. Какие из ниже перечисленных методов относятся к методам одномерной оптимизации?

1). Методы Розенброка, Хука-Дживса, Нелдера-Мида, случайного поиска.

2) Методы быстрого спуска, сопряженных градиентов, переменной метрики.

3) Методы быстрого спуска, Розенброка, Хука-Дживса, метод золотого сечения.

4) Метод дихотомического деления, метод золотого сечения, метод чисел Фибоначчи, метод полиномиальной аппроксимации.

8. Параметрический синтез это..

1) задача оптимизации на базе многовариантного анализа

2) проектировочные процедуры, заключающиеся в разработке или выборе структуры объекта

3) задача оптимизации на базе двовариантного анализа.

4) процедура проектирования, заключающаяся в расчете или выборе значений параметров элементов объекта.

9. В зависимости от количества управляемых параметров методы

оптимизации делятся на методы …

1) одномерной и многомерной оптимизации

2) двумерной и многомерной оптимизации

3) одномерной и n + к-мерной оптимизации

4) одномерной, двумерной и трехмерной

10. Классификация оптимизационных моделей по критерию наличия или отсутствия ограничений…

1) полной и безусловной оптимизации

2) полной и неполной оптимизации

3) условной и безусловной оптимизации

4) условной и частичной оптимизации.

7.2.4Примерныйпереченьвопросовдляподготовкикзачету

Непредусмотреноучебнымпланом

7.2.5Примерныйпереченьзаданийдлярешенияприкладныхзадач

Системный подход к проектированию. Понятие инженерного проектирования. Принципы системного подхода. Основные понятия системотехники. Иерархическая структура проектных спецификаций и иерархические уровни проектирования. Стадии проектирования. Содержание типовых ТЗ. Классификация моделей и параметров, используемых при автоматизированном проектировании информационных систем

Компоненты математического обеспечения. Математические модели в процедурах анализа на макроуровне. Методы и алгоритмы анализа на макроуровне

Математическое обеспечение анализа на микроуровне

Математическое обеспечение анализа на функционально-логическом уровне

Математическое обеспечение анализа на системном уровне. Математическое обеспечение синтеза проектных решений.

Постановка задач параметрического синтеза. Обзор методов оптимизации. Постановка задач структурного синтеза. Методы структурного синтеза

Основные понятия. Распределенная информационная система, ее функции. Полностью неоднородные, частично однородные и однородные распределенные системы обработки данных. Классификация распределенных информационных систем по архитектурным особенностям и по степени распределённости. Способы организации взаимодействия между ЭВМ. Характеристики распределенной информационной системы. Технология «клиент-сервер». Серверы приложений и прикладные протоколы. Представление данных в информационных системах. Логическая, физическая и программная структуры распределенной информационной системы. Назначение и функции элементов этих структур. Концепция взаимодействия открытых систем. Иерархия системы обработки данных: уровень архитектуры системы обработки данных, среда для конечного пользователя и инструментарий прикладного программиста, операционная система, оборудование. Объектно-ориентированные системы. Свойства открытых

систем и объектно-ориентированных систем программирования

Интрасети и Интернет-сети

Локальные сети LAN и глобальные (региональные) сети WAN, сетевые комплексы или объединенные сети. Термины Карта Сетевого Интерфейса, Физический Порт, Интерфейсы. Стандартные обозначения компонентов сетей. Понятие «интрасеть». Различие интрасети и Интернет-сети. Возможности и предоставляемые услуги. Порядок предоставления доступа Виды доступа. Обязанности пользователей. Права и обязанности управления информатизации по администрированию интрасети. Абсолютно упругий и неупругий удар.

Атаки на интрасети и Интернет-сети. Классификация типов удаленных атак на интрасети по степени риска (RiskFactor), по типу атаки (AttackType), по подверженному данной атаке программному обеспечению (PlatformsAffected). Анализ сетевого трафика. Подмена доверенного объекта. Введение ложного объекта компьютерной сети. Отказ в обслуживании (DoS). Сканирование компьютерных сетей. Сети botnet (BlueCoatSecurityLabs). Эволюция угроз. Классификация угроз безопасности Web-приложений. Аутентификация. Авторизация. Атаки на клиентов. Выполнение кода. Разглашение информации. Логические атаки.

Понятие «Система обнаружения вторжений». Функции системы обнаружения вторжений. Виды систем обнаружения вторжений. Пассивные и активные системы обнаружения вторжений. Основные компоненты системы обнаружения вторжений: датчики (сенсоры) и анализаторы.

Принципы функционирования систем обнаружения вторжений

Структура современных систем обнаружения вторжений. Сущность и функции ее подсистем: подсистемы сбора информации, подсистемы анализа и подсистемы представления данных. Анализ недостатков современных систем обнаружения вторжений.

Требования по безопасности информации. Функциональные требования безопасности для систем обнаружения вторжений. Механизмы защиты. Профили защиты системы обнаружения вторжений. Идентификация профиля защиты. Организация профиля защиты.

Методы обнаружения вторжений

Подходы к защите от типовых удаленных атак на интрасети. Методы обнаружения аномалий: моделирование правил, описательная статистика, нейронные сети, моделирование множества состояний, описательная статистика. Методы обнаружения злоупотреблений: моделирование состояний, экспертные системы, моделирование правил, синтаксический анализ. Методы, основанные на моделировании поведения злоумышленника.

Технологии построения систем обнаружения атак

Существующие технологии построения систем обнаружения атак. Технологии обнаружения аномальной деятельности. Статистический анализ компьютерных атак. Анализ систем, использующих сигнатурные методы. Анализ систем, использующих методы поиска аномалий в поведении. Общая оценка современного подхода к обнаружению вторжений. Концепция

обнаружения компьютерных угроз

Стандарты управления информационной безопасностью

Стандарты ISO/IEC 17799:2002 (BS 7799:2000) – ГОСТ Р ИСО/МЭК 17799 «Управление информационной безопасностью — Информационные технологии» (Informationtechnology — Informationsecuritymanagement»)

Повышение эффективности систем обнаружения атак — интегральный подход. Сценарий атаки. Фазы атаки. Схема интегрального обнаружения компьютерных атак. Эффективность проверки правил в системах обнаружения сетевых атак. Требования доверия к безопасности системы обнаружения вторжений. Аудит безопасности. Управление безопасностью.

Администрирование безопасности. Административные, технические (логические) и физические меры. Администрирование информационной системы в целом. Администрирование сервисов безопасности. Аадминистрирование механизмов безопасности. Обязанности и ответственность администратора. Поддержка безопасности в распределенной системе Типичные проблемы безопасности.

7.2.6.Методикавыставленияоценкиприпроведенииипромежуточной аттестации

(Например:Экзаменпроводитсяпотест-билетам,каждыйизкоторыхсодержит10вопросовизадачу.Каждыйправильныйответнавопросвтестеоценивается1баллом,задачаоценивается в10баллов(5балловверноерешениеи5баллов заверныйответ).Максимальноеколичестванабранныхбаллов–20.

1.Оценка«Неудовлетворительно»ставитсявслучае,еслистудентнабрал менее6баллов.

2.Оценка«Удовлетворительно»ставитсявслучае,еслистудентнабралот6до10баллов

3.Оценка«Хорошо»ставитсявслучае,еслистудентнабралот11до15баллов.

4.Оценка«Отлично»ставится,еслистудентнабралот16до20баллов.)

7.2.7Паспортоценочныхматериалов

№п/п	Контролируемыеразделы(темы)дисциплины	Кодконтролируемойкомпетенции	Наименованиеоценочногосредства
1	Принципы системного похода к созданию иисследованиюмоделейавтоматизированныхсистем	ПК-2, ПК-8, ПК-24, ПСК-7.1, ПСК-7.2	Тест, сдача практических работ требования к курсовому проекту
2	Математическое обеспечение анализа и синтеза проектных решений	ПК-2, ПК-8, ПК-24, ПСК-7.1, ПСК-7.2	Тест, сдача практических работ требования к курсовому проекту
3	Принципы проектирования архитектуры и структуры распределенных систем обработки	ПК-2, ПК-8, ПК-24, ПСК-7.1, ПСК-	Тест, сдача практических

	информации	7.2	работ требования к курсовому проекту
4	Атаки на интрасети и интернет-сети	ПК-2, ПК-8, ПК-24, ПСК-7.1, ПСК-7.2	Тест, сдача практических работ требования к курсовому проекту
5	Основы построения систем обнаружения вторжений	ПК-2, ПК-8, ПК-24, ПСК-7.1, ПСК-7.2	Тест, сдача практических работ требования к курсовому проекту
6	Контроль эффективности системы безопасности распределенной информационной системы	ПК-2, ПК-8, ПК-24, ПСК-7.1, ПСК-7.2	Тест, сдача практических работ требования к курсовому проекту

7.3.Методическиематериалы,определяющиепроцедурыоценивания знаний,умений,навыкови(или)опытадеятельности

Тестированиеосуществляется,либоприпомощикомпьютернойсистемытестирования,либосиспользованиемвыданныхтест-заданийнабумажномносителе.Времятестирования30мин.Затемосуществляетсяпроверкатестаэкзаменатором,ивыставляетсяоценкасогласнометодикивыставленияоценкиприпроведении промежуточнойаттестации.

Решениестандартныхзадачосуществляется,либоприпомощикомпьютернойсистемытестирования,либосиспользованиемвыданныхзадачнабумажномносителе.Времярешениязадач30мин.Затемосуществляетсяпроверкарешениязадачэкзаменатором,ивыставляетсяоценка,согласнометодикивыставленияоценкиприпроведенииипромежуточнойаттестации.

Решениеприкладныхзадачосуществляется,либоприпомощикомпьютернойсистемытестирования,либосиспользованиемвыданныхзадачнабумажномносителе.Времярешениязадач30мин.Затемосуществляетсяпроверкарешениязадачэкзаменатором,ивыставляетсяоценка,согласнометодикивыставленияоценкиприпроведенииипромежуточнойаттестации.

Защитакурсовойработы,курсовогопроектаилиотчетаповсемвидампрактикосуществляетсясогласнотребованиям,предъявляемымкработе,описаннымвметодическихматериалах.Примерноевремязащитынаодногостудентасоставля

ет20мин.

8УЧЕБНОМЕТОДИЧЕСКОЕИИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕДИСЦИПЛИНЫ)

8.1Переченьучебнойлитературы,необходимойдляосвоениядисциплины

Основная литература

1.Владимиров И.В.Технический контроль безопасности информационно-телекоммуникационных систем [Электронный ресурс]: Учеб.пособие. - Электрон.текстовые, граф. дан. (586 кб). - Воронеж: ФГБОУ ВПО "Воронежский государственный технический университет", 2012. - 1 файл. - 30-00.

2. Язов, Ю.К. Технология проектирования систем защиты информации в информационно-телекоммуникационных системах [Электронный ресурс] : учеб.пособие. - Электрон.дан. (1 файл). - Воронеж : ВГТУ, 2004. - 1 электрон.опт. диск (CD-ROM). - 30.00.

Дополнительная литература

1.Ключев А.О. Распределенные информационно-управляющие системы [Электронный ресурс]: учебное пособие/ Ключев А.О., Кустарев П.В., Платунов А.Е.— Электрон.текстовые данные.— Санкт-Петербург: Университет ИТМО, 2015.— 58 с.— Режим доступа: http://www.iprbookshop.ru/68081.html.— ЭБС «IPRbooks».

2.Пелешенко В.С. Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления [Электронный ресурс]: учебное пособие/ Пелешенко В.С., Говорова С.В., Лапина М.А.— Электрон.текстовые данные.— Ставрополь: Северо-Кавказский федеральный университет, 2017.— 86 с.— Режим доступа: http://www.iprbookshop.ru/69405.html.— ЭБС «IPRbooks».

3. Комплексное обеспечение информационной безопасности автоматизированных систем [Электронный ресурс]: лабораторный практикум/ М.А. Лапина [и др.].— Электрон.текстовые данные.— Ставрополь: Северо-Кавказский федеральный университет, 2016.— 242 с.— Режим доступа: http://www.iprbookshop.ru/62945.html.— ЭБС «IPRbooks».

8.2Переченьинформационныхтехнологий,используемыхприосуществлениииобразовательногопроцессаподисциплине,включаяпереченьлицензионногопрограммногообеспечения,ресурсовинформационно-телекоммуникационнойсети«Интернет»,современныхпрофессиональныхбазданныхиинформационныхсправочныхсистем:

http://att.nica.ru
http://www.edu.ru/
http://window.edu.ru/window/library
http://www.intuit.ru/catalog/
http://bibl.cchgeu.ru/MarcWeb2/ExtSearch.asp
https://cchgeu.ru/education/cafedras/kafsib/?docs
http://www.eios.vorstu.ru

http://e.lanbook.com/ (ЭБС Лань)
http://IPRbookshop.ru/ (ЭБСIPRbooks)

9МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯБАЗА,НЕОБХОДИМАЯДЛЯОСУЩЕСТВЛЕНИЯОБРАЗОВАТЕЛЬНОГОПРОЦЕССА

Специализированная лекционная аудитория, оснащенная оборудованием для лекционных демонстраций и проекционной аппаратурой, а так же учебная аудитория для проведения занятий лабораторного типа.

10.МЕТОДИЧЕСКИЕУКАЗАНИЯДЛЯОБУЧАЮЩИХСЯПООСВОЕНИЮДИСЦИПЛИНЫ(МОДУЛЯ)

Подисциплине«Информационнаябезопасностираспределённыхинформационныхсистем»читаютсялекции,проводятсялабораторныеработы,выполняетсякурсовойпроект.

Основойизучениядисциплиныявляютсялекции,накоторыхизлагаютсяналиболеесущественныеитрудныевопросы,атакжевопросы,ненашедшиеотражениявучебнойлитературе.

Лабораторныеработывыполняютсяналабораторномоборудованиивсоответствиисметодиками,приведеннымивуказанияхквыполнениюработ.

Методикавыполнениякурсовогопроектаизложенавучебно-методическомпособии.Выполнятьэтапыкурсовогопроектадолжнысвоевременноивустановленныесроки.

Контрольусвоенияматериаладисциплиныпроизводитсяпроверкойкурсовогопроекта,защитойкурсовогопроекта.

Видучебныхзанятий	Деятельностьстудента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначение вопросов, терминов, материала, которые вызывают трудности, поиск ответов в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на лекции или на практическом занятии.
Лабораторнаяработа	Лабораторные работы позволяют научиться применять теоретические знания, полученные на лекции при решении конкретных задач. Чтобы наиболее рационально и полно использовать все возможности лабораторных для подготовки к ним необходимо: следует разобрать лекцию по соответствующей теме, ознакомится с соответствующим разделом учебника, проработать дополнительную литературу и источники, решить задачи и выполнить другие письменные задания.
Самостоятельнаяработа	Самостоятельная работа студентов способствует глубокому усвоения учебного материала и развитию навыков самообразования. Самостоятельная работа предполагает

	следующие составляющие: - работа с текстами: учебниками, справочниками, дополнительной литературой, а также проработка конспектов лекций; - выполнение домашних заданий и расчетов; - работа над темами для самостоятельного изучения; - участие в работе студенческих научных конференций, олимпиад; - подготовка к промежуточнойаттестации.
Подготовка к промежуточнойаттестации	Готовиться к промежуточной аттестации следует систематически, в течение всего семестра. Интенсивная подготовка должна начаться не позднее, чем за месяц-полтора до промежуточной аттестации. Данные перед экзаменом три дня эффективнее всего использовать для повторения и систематизации материала.