

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

ПРИЕМ 2018 г.

ФОРМА ОБУЧЕНИЯ очная

Администрирование вычислительных сетей и систем

Направление подготовки/ специальность	09.03.02 Информационные системы и технологии		
Образовательная программа (направленность (профиль))	Информационные системы и технологии в бизнесе и промышленности		
	Информационные системы и технологии в бизнесе		
Уровень образования	высшее образование - бакалавриат		
Курс	4	семестр	8
Трудоемкость в кредитах (зачетных единицах)	3		

Заведующий кафедрой -
руководитель отделения на
правах кафедры
Руководитель ООП
Преподаватель

	Шерстнев В.С.
	Цапко И.В.
	Фадеев А.С.

2020 г.

1. Роль дисциплины «Администрирование вычислительных сетей и систем» в формировании компетенций выпускника:

Элемент образовательной программы (дисциплина, практика, ГИА)	Семестр	Код компетенции	Наименование компетенции	Индикаторы достижения компетенций		Составляющие результатов освоения (дескрипторы компетенций)	
				Код индикатора	Наименование индикатора достижения	Код	Наименование
Администрирование вычислительных сетей и систем	8	ПК(У)-3	Способен создавать техническую документацию на продукцию в сфере информационных технологий, управлять технической информацией	И.ПК(У)-3.1	Демонстрирует способность разрабатывать технические спецификации на программные компоненты и их взаимодействие	ПК(У)-3.1У2	Умеет активизировать, конфигурировать, документировать и контролировать работу стандартные сервисы сетевых операционных систем
						ПК(У)-3.132	Знает основные протоколы и сервисы сети Интернет
		ПК(У)-4	Способен выполнять работы по обеспечению функционирования баз данных и обеспечению их информационной безопасности	И.ПК(У)-4.2	Демонстрирует способность осуществлять администрирование информационных систем и обеспечивать безопасность на уровне БД	ПК(У)-4.2В1	Владеет методами проектирования, развертывания и администрирования информационных систем
						ПК(У)-4.2У1	Умеет проектировать, устанавливать и настраивать службы безопасности, организации доступа, именования и адресации
						ПК(У)-4.231	Знает способы проектирования компонентов информационных систем;
						ПК(У)-4.2В2	Владеет методами анализа, управления и контроля за состоянием работающих информационных систем
						ПК(У)-4.2У2	Умеет анализировать состояния и функционирования систем и информационных потоков
						ПК(У)-4.232	Знает методы администрирования и контроля; возможностей платформ, средств и систем администрирования

2. Показатели и методы оценивания

Планируемые результаты обучения по дисциплине		Код контролируемой компетенции (или ее части)	Наименование раздела дисциплины	Методы оценивания (оценочные мероприятия)
Код	Наименование			
РД1	Знания: Методов администрирования и контроля; возможностей платформ, средств и систем администрирования; функционирования основных протоколов и сервисов Интернета.	И.ПК(У)-4.2	Раздел 1. Информационная модель TCP/IP Раздел 2. Сетевое взаимодействие	Тестирование Контрольная работа
РД2	Умения: Активизировать, конфигурировать и контролировать работу сервисов сетевых операционных систем; анализировать состояния и функционирования систем и информационных потоков.	И.ПК(У)-3.1	Раздел 2. Сетевое взаимодействие	Тестирование Case-study
РД3	Владение: Навыками администрирования информационных систем.	И.ПК(У)-4.2	Раздел 1. Информационная модель TCP/IP	Контрольная работа

			Раздел 2. Сетевое взаимодействие Раздел 3. Низкоуровневая обработка пакетов	

3. Шкала оценивания

Порядок организации оценивания результатов обучения в университете регламентируется отдельным локальным нормативным актом – «Система оценивания результатов обучения в Томском политехническом университете (Система оценивания)» (в действующей редакции). Используется балльно-рейтинговая система оценивания результатов обучения. Итоговая оценка (традиционная и литерная) по видам учебной деятельности (изучение дисциплин, УИРС, НИРС, курсовое проектирование, практики) определяется суммой баллов по результатам текущего контроля и промежуточной аттестации (итоговая рейтинговая оценка – максимум 100 баллов).

Распределение основных и дополнительных баллов за оценочные мероприятия текущего контроля и промежуточной аттестации устанавливается календарным рейтинг-планом дисциплины.

Рекомендуемая шкала для отдельных оценочных мероприятий входного и текущего контроля

% выполнения задания	Соответствие традиционной оценке	Определение оценки
90%÷100%	«Отлично»	Отличное понимание предмета, всесторонние знания, отличные умения и владение опытом практической деятельности, необходимые результаты обучения сформированы, их качество оценено количеством баллов, близким к максимальному
70% - 89%	«Хорошо»	Достаточно полное понимание предмета, хорошие знания, умения и опыт практической деятельности, необходимые результаты обучения сформированы, качество ни одного из них не оценено минимальным количеством баллов
55% - 69%	«Удовл.»	Приемлемое понимание предмета, удовлетворительные знания, умения и опыт практической деятельности, необходимые результаты обучения сформированы, качество некоторых из них оценено минимальным количеством баллов
0% - 54%	«Неудовл.»	Результаты обучения не соответствуют минимально достаточным требованиям

Шкала для оценочных мероприятий экзамена

% выполнения заданий экзамена	Экзамен, балл	Соответствие традиционной оценке	Определение оценки
90%÷100%	18 ÷ 20	«Отлично»	Отличное понимание предмета, всесторонние знания, отличные умения и владение опытом практической деятельности, необходимые результаты обучения сформированы, их качество оценено количеством баллов, близким к максимальному
70% - 89%	14 ÷ 17	«Хорошо»	Достаточно полное понимание предмета, хорошие знания, умения и опыт практической деятельности, необходимые результаты обучения сформированы, качество ни одного из них не оценено минимальным количеством баллов
55% - 69%	11 ÷ 13	«Удовл.»	Приемлемое понимание предмета, удовлетворительные знания, умения и опыт практической деятельности, необходимые результаты обучения сформированы, качество некоторых из них оценено минимальным количеством баллов

4. Перечень типовых заданий

Оценочные мероприятия		Примеры типовых контрольных заданий																												
1.	Тестирование	A B C D - o - o - o - o - Ethernet 1 IP - сеть "development" E F G - o - o - o - o - Ethernet 2 IP - сеть "accounting" D H I J - o - o - o - o - Ethernet 3 IP - сеть "factory" 1. <u>Пакет</u> движется по сети, указанной на рисунке, от узла В к узлу Н и его перехватывает хакер на узле С. MAC-адрес какого узла будет указан в заголовке <u>Ethernet-протокола</u> в качестве отправителя? Для ответа введите букву-имя компьютера. Ответ: 2. <u>Динамическая</u> таблица соответствия, сформированная на пограничном <u>шлюзе</u>, использующем службу <u>NAPT</u>, имеет вид: <table><tr><th>Приватный IP</th><th>Приватный № порта</th><th>Протокол</th><th>Публичный № порта</th></tr><tr><td>192.168.0.13</td><td>1964</td><td>TCP</td><td>2424</td></tr><tr><td>192.168.0.166</td><td>16384</td><td>TCP</td><td>17569</td></tr><tr><td>192.168.0.21</td><td>9599</td><td>TCP</td><td>14006</td></tr><tr><td>192.168.0.33</td><td>17569</td><td>TCP</td><td>16384</td></tr><tr><td>192.168.0.36</td><td>2424</td><td>TCP</td><td>13013</td></tr><tr><td>192.168.0.111</td><td>1026</td><td>TCP</td><td>1964</td></tr></table> Публичный <u>IP</u>-адрес пограничного <u>шлюза</u>: 109.123.140.100. Какой исходящий порт будет указан у <u>пакета</u>, отправленного узлом 192.168.0.21, и перехваченного в	Приватный IP	Приватный № порта	Протокол	Публичный № порта	192.168.0.13	1964	TCP	2424	192.168.0.166	16384	TCP	17569	192.168.0.21	9599	TCP	14006	192.168.0.33	17569	TCP	16384	192.168.0.36	2424	TCP	13013	192.168.0.111	1026	TCP	1964
Приватный IP	Приватный № порта	Протокол	Публичный № порта																											
192.168.0.13	1964	TCP	2424																											
192.168.0.166	16384	TCP	17569																											
192.168.0.21	9599	TCP	14006																											
192.168.0.33	17569	TCP	16384																											
192.168.0.36	2424	TCP	13013																											
192.168.0.111	1026	TCP	1964																											

	Оценочные мероприятия	Примеры типовых контрольных заданий								
		публичной сети? Ответ: 3. Какие параметры необходимо настроить на <u>клиентском</u> программном обеспечении для подключения ко внешним <u>серверам</u>, если в локальной сети используется "прозрачный <u>прокси</u>" для выхода в Интернет? Выберите один ответ: ☐ а. <u>IP-адрес прокси-сервера</u>, номер порта <u>прокси-сервера</u> и тип <u>прокси</u> ☐ б. <u>IP-адрес прокси-сервера</u> и номер порта <u>прокси-сервера</u> ☐ в. <u>IP-адрес маршрутизатора</u> и номер порта <u>маршрутизатора</u>, который пересылает данные на <u>прокси</u> ☐ г. Никаких, всю работу выполнит <u>маршрутизатор</u>								
2.	Контрольная работа	Контрольная работа: При выполнении работы, считать, что: – все сети класса «С»; – приватная сеть использует приватные адреса; – физические соединения внутри каждой сети реализованы через прозрачные для узлов коммутаторы; – маскардинг организован по технологии NAPT; – Внутренний IP-адрес шлюза задается по следующему правилу: X.Y.Z.W, где X – произвольное число, Y=двум первым цифрам номера группы студента, Z=номеру студента в группе, W=1. Задания: 1. Определите количество сетей (подсетей), обозначьте их границы на рисунке; 2. Подпишите IP-адрес и маску для каждой сети (подсети); 2.1. Каждому узлу сети подпишите его IP-адрес в формате «.XX». 3. Для узлов «Ai» и «Bi» (i=номеру студента в группе), составьте и запишите полные таблицы маршрутизации, описывающие для этих узлов маршруты: 3.1. к каждой из изображенных подсетей; 3.2. к своей подсети; 3.3. к самому себе; 3.4. к узлу localhost 3.5. ко всем узлам Интернета. «Ai» <table><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr></table>								

	Оценочные мероприятия	Примеры типовых контрольных заданий			
		«Vi»			
		...			
		7. В таблице приведен список правил брандмауэра IPFW, установленного на пограничном маршрутизаторе вымышленной локальной сети. Маршрутизатор оснащен четырьмя сетевыми интерфейсами: – lif и wifi-if – интерфейсы в локальную сеть с приватными адресами. – pif – интерфейс в публичную сеть с «белым» ip-адресом. – lo0 – локальная петля localhost. Опишите полный путь прохождения пакета-запроса от узла локальной приватной сети к веб-серверу ya.ru и ответа на этот запрос: укажите по шагам, через какие процедуры обработки внутри ядра проходят пакеты, какие мета-теги появляются у пакетов, какие правила срабатывают для пакета.			
		005 allow all from any to any in recv \$lif			
		006 allow all from any to any in recv \$wifi-if			
		010 allow all from any to any via lo0			
		014 divert natd ip from any to any in via \$pif			
		015 check-state			
		020 skipto 800 tcp from any to any 53 out via \$pif keep-state			
		020 skipto 800 udp from any to any 53 out via \$pif keep-state			
		040 skipto 800 tcp from any to any 80 out via \$pif setup keep-state			
		060 skipto 800 tcp from any to any 25 out via \$pif setup keep-state			
		061 skipto 800 tcp from any to any 110 out via \$pif setup keep-state			
		070 skipto 800 tcp from me to any out via \$pif setup keep-state			
		130 skipto 800 icmp from any to any out via \$pif keep-state			
		140 skipto 800 icmp from any to me icmptype 0,3,8,11			
		150 skipto 800 udp from any to any 123 out via \$pif keep-state			
		300 deny all from 192.168.0.0/16 to any in via \$pif			
		301 deny all from 172.16.0.0/12 to any in via \$pif			
		302 deny all from 10.0.0.0/8 to any in via \$pif			

	Оценочные мероприятия	Примеры типовых контрольных заданий
		303 deny all from 127.0.0.0/8 to any in via \$pif 304 deny all from 0.0.0.0/8 to any in via \$pif 305 deny all from 169.254.0.0/16 to any in via \$pif 306 deny all from 192.0.2.0/24 to any in via \$pif 307 deny all from 204.152.64.0/23 to any in via \$pif 308 deny all from 224.0.0.0/3 to any in via \$pif 330 deny all from any to any frag in via \$pif 332 deny tcp from any to any established in via \$pif #340 deny tcp from any to any 137 in via \$pif #341 deny tcp from any to any 138 in via \$pif #342 deny tcp from any to any 139 in via \$pif 350 allow all from any to any out via \$lif 353 allow all from any to any out via \$wifi-if 360 allow tcp from any to me 53 in via \$pif setup limit src-addr 2 361 allow udp from any to me 53 in via \$pif limit src-addr 2 370 allow tcp from any to me 80 in via \$pif setup limit src-addr 15 380 allow tcp from any to me 22 in via \$pif limit src-addr 10 400 deny log all from any to any in via \$pif 450 deny log all from any to any out via \$pif 800 divert natd ip from any to any out via \$pif 801 allow ip from any to any 999 deny log all from any to any
3.	Задание case-study	Задание: Представьте ситуацию: вы попали на работу в небольшую компанию. Кто-то с друзьями открыл ООО, кто-то сам создал ИП, кто-то удачно вышел за муж и уехал в Дальнеуральск-уездный и там пришел работать в компанию, а кого-то забрали в армию, а там, всяко, лучше быть админом, чем бакланом... Не важно как и в какую. Но вот так случилось. Вы попали... Народу (адекватного, умеющего писать макросы на Экселе) в компании не много (неадекватного - больше). Компьютеров, штук 20. Выход в интернет проводной один. Ясно, что IP-адрес белый тоже только один. И есть LTE-модем с конскими тарифами на интернет. Когда интернет пропадает, модем втыкают в компьютер того, кому больше всех надо, и у него случается счастье. Есть три сетевых принтера. 4 ноутбука. 1 wi-fi-роутер, коммутаторы в каждом кабинете и расшаренные диски "Службы доступа к файлам и принтерам Microsoft", которые доступны, пока нужные компьютеры включены. и "Всё вроде бы ровно, но..." Всё работает ужасно медленно. Отваливается интернет. Половина компьютеров друг друга не видят в сети. Роутер через день зависает. А еще, сотрудники вывалили на облачное хранилище за пределами компании файлы с коммерческой тайной, чтобы хоть как-то иметь к ним доступ и начальство боится, что за ним скоро придут вежливые люди. Но кроме всего этого руководство требует от Вас сделать так,

	Оценочные мероприятия	Примеры типовых контрольных заданий
		чтобы: – Все важные документы должны быть доступны с любого компьютера компании круглосуточно и должны резервироваться; – Руководство (и не только) должно иметь возможность работать с некоторыми документами из дома; – При отключении интернета должен работать резервный канал через сотовую связь; – Сотрудники (кроме руководителей) должны иметь возможность работать с любого компьютера организации и получать доступ к своим файлам; – Должен быть собственный сайт с простым именем русскими буквами, собственная электронная почта; – Политика фирмы не разрешает заходить сотрудникам на страницы соцсетей: соцсети просто недоступны, вместо них открывается собственный сайт компании. Но руководству можно и в соцсети. – Нужен телеграм. Нужен на каждом компьютере. Но провайдером интернета он заблокирован. Есть еще и требования для вас, как для администратора: – возможность из дома управлять всеми настройками сетевой и серверной конфигурации; – возможность из дома подключаться к любому компьютеру компании через "Удаленный помощник" или "Удаленное подключение к рабочему столу"; – необходимо обезопасить всю сеть от возможного взлома публичных серверов (а он точно будет случаться, и будет случаться часто); доступ к Wi-Fi для гостей компании должен быть открыт, но должен вести только на сайт компании.

5. Методические указания по процедуре оценивания

Оценочные мероприятия		Процедура проведения оценочного мероприятия и необходимые методические указания
1.	Тестирование	За каждый правильный ответ – 1 балл.
2.	Контрольная работа	Задание на работу вложено в виде файла форматов .doc и .pdf. Каждый студент, должен выполняя задания, вписывать значение в файл. При необходимости, файл можно снабдить комментариями. Итоговый файл с результатами необходимо загрузить на проверку до истечения контрольного срока. При правильном выполнении заданий они оцениваются следующим образом: 1 балл 1 балл 1 балл 1 балл 2 балла 2 балла 5 баллов
3.	Задание case-study	- За предложенный концепт работоспособного решения каждой отдельной задачи - 1 балл. Концепт должен описывать технологию, <u>протоколы</u>, параметры (объем, скорость, <u>вместимость</u>, количество портов и т.д.) ограничения её применения и обоснование выбора. - За детализацию настроек с точностью до адресов, номеров портов, имен, правил и конкретных параметров - еще +1 балл. - За работающую конфигурацию по каждой задаче +5 баллов. - За каждую неявную задачу, без которых решение кейса невозможно, расценки такие же, как в п.1. - За работающую конфигурацию нескольких задач одновременно, добавляются баллы по формуле $B = n * n / 2 - 1$, где Б - количество дополнительных баллов, n - количество задач, реально работающих одновременно. - Если решение потенциально уязвимо для примитивных атак - задание не засчитывается. - За плагиат баллы вычитаются, но по тем же формулам и законам. - За оригинальность, красоту, эстетику, и вау-вау, баллы могут быть добавлены на основе взаимного согласования.