МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ»
(ТУСУР)

УТВЕРЖДАЮ
Директор департамента образования

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Информационная безопасность в локальных и распределенных вычислительных сетях

Уровень образования: **высшее образование - специалитет**
Направление подготовки / специальность: **38.05.01 Экономическая безопасность**
Специализация: **Экономико-правовое обеспечение экономической безопасности**
Направленность (профиль): **Проектная деятельность при обеспечении экономической и информационной безопасности**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**
Курс: **4**
Семестр: **8**
Учебный план набора 2016 года

Распределение рабочего времени

№	Виды учебной деятельности	8 семестр	Всего	Единицы
1	Лекции	36	36	часов
2	Практические занятия	72	72	часов
3	Всего аудиторных занятий	108	108	часов
4	Самостоятельная работа	108	108	часов
5	Всего (без экзамена)	216	216	часов
6	Общая трудоемкость	216	216	часов
		6.0	6.0	З.Е.

Дифференцированный зачет: 8 семестр

Томск 2018

Рассмотрена и одобрена на заседании кафедры
протокол № 6 от «15» 5 2018 г.

ЛИСТ СОГЛАСОВАНИЯ

Рабочая программа дисциплины составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 38.05.01 Экономическая безопасность, утвержденного 16.01.2017 года, рассмотрена и одобрена на заседании кафедры КИБЭВС «___» _____ 20__ года, протокол №_____.

Разработчик:

Старший преподаватель каф.
КИБЭВС _____ Г. А. Праскурин

Заведующий обеспечивающей каф.
КИБЭВС _____ А. А. Шелупанов

Рабочая программа дисциплины согласована с факультетом и выпускающей кафедрой:

Декан ФБ _____ Е. М. Давыдова

Заведующий выпускающей каф.
КИБЭВС _____ А. А. Шелупанов

Эксперты:

Доцент каф.КИБЭВС _____ А. А. Конев
Доцент каф.КИБЭВС _____ К. С. Сарин

1. Цели и задачи дисциплины

1.1. Цели дисциплины

подготовка слушателей основам эксплуатации вычислительных сетей, принципам и методам защиты информации в компьютерных сетях, навыкам комплексного проектирования, построения, обслуживания и анализа защищенных вычислительных сетей, а так же содействие фундаментализации образования, формированию научного мировоззрения и развитию системного мышления.

1.2. Задачи дисциплины

- Изучение основных понятий информационной безопасности;
- Изучение угроз безопасност информации в вычислительных сетях;
- Изучение технологий обеспечения безопасности информации;
- Изучение механизмов обеспечения безопасности информации в локальных сетях;
- Изучение механизмов обеспечения безопасности нформации при межсетевом взаимодействии;
- Изучение правовых основ защиты информации в вычислительных сетях.

2. Место дисциплины в структуре ОПОП

Дисциплина «Информационная безопасность в локальных и распределенных вычислительных сетях» (Б1.В.ДВ.4.1) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Операционные системы, Организационное и правовое обеспечение информационной безопасности, Основы информационной безопасности.

Последующими дисциплинами являются: Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты, Управление информационной безопасностью.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- ПСК-2 способностью выявлять условия, способствующие совершению правонарушений в отношении сведений, составляющих государственную, банковскую, коммерческую тайну, персональных данных, других сведений ограниченного доступа;

В результате изучения дисциплины обучающийся должен:

- **знать** - эталонную модель взаимодействия открытых систем; - основные стандарты в области инфокоммуникационных систем и технологий; - принципы построения защищенных телекоммуникационных систем; - механизмы реализации атак в компьютерных сетях; - защитные механизмы и средства обеспечения сетевой безопасности; - средства и методы предотвращения и обнаружения вторжений.
- **уметь** - применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях; - осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты.
- **владеть** - навыками конфигурирования локальных сетей, реализации сетевых протоколов с помощью программных средств; - навыками настройки межсетевых экранов; - методикой анализа сетевого трафика; - методикой анализа результатов работы средств обнаружения вторжений.

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 6.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры
		8 семестр

Аудиторные занятия (всего)	108	108
Лекции	36	36
Практические занятия	72	72
Самостоятельная работа (всего)	108	108
Проработка лекционного материала	48	48
Подготовка к практическим занятиям, семинарам	60	60
Всего (без экзамена)	216	216
Общая трудоемкость, ч	216	216
Зачетные Единицы	6.0	6.0

5. Содержание дисциплины

5.1. Разделы дисциплины и виды занятий

Разделы дисциплины и виды занятий приведены в таблице 5.1.

Таблица 5.1 – Разделы дисциплины и виды занятий

Названия разделов дисциплины	Лек., ч	Прак. зан., ч	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
8 семестр					
1 Основные понятия вычислительных сетей	4	4	12	20	ПСК-2
2 Основные понятия информационной безопасности	4	4	12	20	ПСК-2
3 Угрозы безопасности информации в вычислительных сетях	2	4	8	14	ПСК-2
4 Технологии обеспечения безопасности информации в вычислительных сетях	4	4	8	16	ПСК-2
5 Обеспечение безопасности информации в локальных сетях	4	14	16	34	ПСК-2
6 Обеспечение безопасности информации при межсетевом взаимодействии	14	34	40	88	ПСК-2
7 Правовые основы защиты информации в вычислительных сетях	4	8	12	24	ПСК-2
Итого за семестр	36	72	108	216	
Итого	36	72	108	216	

5.2. Содержание разделов дисциплины (по лекциям)

Содержание разделов дисциплин (по лекциям) приведено в таблице 5.2.

Таблица 5.2 – Содержание разделов дисциплин (по лекциям)

Названия разделов	Содержание разделов дисциплины (по лекциям)	Трудоемкость, ч	Формируемые компетенции

8 семестр			
1 Основные понятия вычислительных сетей	Предмет, цель и содержание дисциплины. Место и роль вычислительных сетей в современном мире. Общие представления о вычислительной сети. Вычислительные сети и распределенные системы.Принципы многоуровневой организации локальных и глобальных сетей ЭВМ. Модель OSI. Уровни модели OSI. Стандартные стеки коммуникационных протоколов.	2	ПСК-2
	Основное коммуникационное оборудование (сетевые адаптеры и концентраторы, мосты и коммутаторы, маршрутизаторы).Технология Ethernet (IEEE802.3).Построение сетей на основе сетевого уровня.Реализация межсетевого взаимодействия средствами TCP/IP. Протоколы IP, UDP, TCP. Протоколы прикладного уровня.	2	
	Итого	4	
2 Основные понятия информационной безопасности	Основные понятия в области информационной безопасности. Конфиденциальность, целостность, доступность информации (информационного ресурса).Понятия угроза, уязвимость, атака. Классификация угроз. Источники угроз. Классификация уязвимостей. Источники уязвимостей. База уязвимостей CVE.Классификация атак. Типовой сценарий реализации атак.	2	ПСК-2
	Примеры реализации сетевых атак.Типовой сценарий реализации сетевых атак.	2	
	Итого	4	
3 Угрозы безопасности информации в вычислительных сетях	Специфические угрозы при подключении узлов к вычислительной сети.Уязвимости протоколов сетевого взаимодействия и распределенных информационных систем.Типовые атаки на локальные и распределенные вычислительные сети.	2	ПСК-2
	Итого	2	
4 Технологии обеспечения безопасности информации в вычислительных сетях	Базовые механизмы защиты информации в локальных и глобальных сетях.Разграничение доступа к сетевым ресурсам. Межсетевое экранирование. Антивирусная защита. Виртуальные честные сети (VPN).Дополнительные механизмы защиты в локальных и глобальных	4	ПСК-2
	Итого	4	
5 Обеспечение безопасности информации в локальных сетях	Защита от несанкционированного доступа к узлам и информационным ресурсам в локальных сетях.Ограничение доступа к сетевым установсикам средствами операционной системы хоста.Предотвращение утечки информации в результате действий внутренних злоумышленников.	4	ПСК-2
	Итого	4	
6 Обеспечение	Защита периметра информационной системы меж-	14	ПСК-2

безопасности информации при межсетевом взаимодействии	сетевыми экранами. Понятие демилитаризованной зоны.Атнивирусная защита компьютерных сете.Обнаружение и предоьвращение вторжений. Классификация систем обнаружения вторжени.Применение технологии виртуальных частных сетей для защиты каналов связи компьютерных сетей. Основные компоненты VPN. Сканирование ресурсов и узолов сети на наличие уязвимостей и соответствие требованиям нормативных документов по защите информации.Современные технологии защиты информации в компьютерных сетях. Технология NGFW. Защита информации в виртуальной инфраструктуре.		
	Итого	14	
7 Правовые основы защиты информации в вычислительных сетях	Требования нормативных документов по защите персональных данных при обработке и перевысле в локальных и глобальных сетях.Требования нормативных документов по защите конфиденциальной информации.Управление информационной безопасностью компьютерынх сетей.	4	ПСК-2
	Итого	4	
Итого за семестр		36	

5.3. Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами

Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами представлены в таблице 5.3.

Таблица 5.3 – Разделы дисциплины и междисциплинарные связи

Наименование дисциплин	№ разделов данной дисциплины, для которых необходимо изучение обеспечивающих и обеспечиваемых дисциплин						
	1	2	3	4	5	6	7
Предшествующие дисциплины							
1 Операционные системы	+						
2 Организационное и правовое обеспечение информационной безопасности	+	+	+	+			
3 Основы информационной безопасности		+	+	+			
Последующие дисциплины							
1 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты		+	+	+	+	+	+
2 Управление информационной безопасностью				+	+	+	+

5.4. Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий представлено в таблице 5.4.

Таблица 5.4 – Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Компетенции	Виды занятий			Формы контроля
	Лек.	Прак. зан.	Сам. раб.	
ПСК-2	+	+	+	Опрос на занятиях, Тест, Дифференцированный зачет, Отчет по практическому занятию

6. Интерактивные методы и формы организации обучения

Не предусмотрено РУП.

7. Лабораторные работы

Не предусмотрено РУП.

8. Практические занятия (семинары)

Наименование практических занятий (семинаров) приведено в таблице 8.1.

Таблица 8.1 – Наименование практических занятий (семинаров)

Названия разделов	Наименование практических занятий (семинаров)	Трудоемкость, ч	Формируемые компетенции
8 семестр			
1 Основные понятия вычислительных сетей	Настройка подключения хоста к локальной сети. Базовые службы локальных и шлобальных сетей.	4	ПСК-2
	Итого	4	
2 Основные понятия информационной безопасности	Анализ угроз безопасности информации и их источников. Планирование структуры системы защиты информации	4	ПСК-2
	Итого	4	
3 Угрозы безопасности информации в вычислительных сетях	Анализ угроз безопасности информации в системе. Составление модели угроз.	4	ПСК-2
	Итого	4	
4 Технологии обеспечения безопасности информации в вычислительных сетях	Планирование структуры системы защиты информации в компьютерной сети. Обоснование выбоора методов и средств защиты информации.	4	ПСК-2
	Итого	4	
5 Обеспечение безопасности информации в локальных сетях	Защита информации от несанкционированного доступа штатными и дополнительными средствами операционных систем	4	ПСК-2
	Разграничение доступа к сетевым устройствам, хостам и информационным ресурсам локальной сети	6	
	DLP-системы.	4	
	Итого	14	
6 Обеспечение	Межсетевые экраны	6	ПСК-2

безопасности информации при межсетевом взаимодействии	Системы обнаружения и предотвращения вторжений.	6	
	Технология VPN.	6	
	Сканеры безопасности	6	
	Антивирусная защита	6	
	Защита информации в виртуальной инфраструктуре.	4	
	Итого	34	
7 Правовые основы защиты информации в вычислительных сетях	Защита персональных данных в соответствии с требованиями нормативных документов	4	ПСК-2
	Защита конфиденциальной информации в соответствии с требованиями нормативных документов	4	
	Итого	8	
Итого за семестр		72	

9. Самостоятельная работа

Виды самостоятельной работы, трудоемкость и формируемые компетенции представлены в таблице 9.1.

Таблица 9.1 – Виды самостоятельной работы, трудоемкость и формируемые компетенции

Названия разделов	Виды самостоятельной работы	Трудоемкость, ч	Формируемые компетенции	Формы контроля
8 семестр				
1 Основные понятия вычислительных сетей	Подготовка к практическим занятиям, семинарам	4	ПСК-2	Дифференцированный зачет, Опрос на занятиях, Тест
	Проработка лекционного материала	4		
	Проработка лекционного материала	4		
	Итого	12		
2 Основные понятия информационной безопасности	Подготовка к практическим занятиям, семинарам	4	ПСК-2	Дифференцированный зачет, Опрос на занятиях, Тест
	Проработка лекционного материала	4		
	Проработка лекционного материала	4		
	Итого	12		
3 Угрозы безопасности информации в вычислительных сетях	Подготовка к практическим занятиям, семинарам	4	ПСК-2	Дифференцированный зачет, Опрос на занятиях, Тест
	Проработка лекционного материала	4		

	Итого	8		
4 Технологии обеспечения безопасности информации в вычислительных сетях	Подготовка к практическим занятиям, семинарам	4	ПСК-2	Дифференцированный зачет, Опрос на занятиях, Тест
	Проработка лекционного материала	4		
	Итого	8		
5 Обеспечение безопасности информации в локальных сетях	Подготовка к практическим занятиям, семинарам	12	ПСК-2	Дифференцированный зачет, Опрос на занятиях, Тест
	Проработка лекционного материала	4		
	Итого	16		
6 Обеспечение безопасности информации при межсетевом взаимодействии	Подготовка к практическим занятиям, семинарам	24	ПСК-2	Дифференцированный зачет, Опрос на занятиях, Тест
	Проработка лекционного материала	16		
	Итого	40		
7 Правовые основы защиты информации в вычислительных сетях	Подготовка к практическим занятиям, семинарам	8	ПСК-2	Дифференцированный зачет, Опрос на занятиях, Тест
	Проработка лекционного материала	4		
	Итого	12		
Итого за семестр		108		
Итого		108		

10. Курсовой проект / курсовая работа

Не предусмотрено РУП.

11. Рейтинговая система для оценки успеваемости обучающихся

11.1. Балльные оценки для элементов контроля

Таблица 11.1 – Балльные оценки для элементов контроля

Элементы учебной деятельности	Максимальный балл на 1-ую КТ с начала семестра	Максимальный балл за период между 1КТ и 2КТ	Максимальный балл за период между 2КТ и на конец семестра	Всего за семестр
8 семестр				
Дифференцированный зачет			30	30
Опрос на занятиях	5	5	10	20
Отчет по практическому занятию	5	5	10	20
Тест	10	10	10	30
Итого максимум за пери-	20	20	60	100

од				
Нарастающим итогом	20	40	100	100

11.2. Пересчет баллов в оценки за контрольные точки

Пересчет баллов в оценки за контрольные точки представлен в таблице 11.2.

Таблица 11.2 – Пересчет баллов в оценки за контрольные точки

Баллы на дату контрольной точки	Оценка
≥ 90% от максимальной суммы баллов на дату КТ	5
От 70% до 89% от максимальной суммы баллов на дату КТ	4
От 60% до 69% от максимальной суммы баллов на дату КТ	3
< 60% от максимальной суммы баллов на дату КТ	2

11.3. Пересчет суммы баллов в традиционную и международную оценку

Пересчет суммы баллов в традиционную и международную оценку представлен в таблице 11.3.

Таблица 11.3 – Пересчет суммы баллов в традиционную и международную оценку

Оценка (ГОС)	Итоговая сумма баллов, учитывает успешно сданный экзамен	Оценка (ECTS)
5 (отлично) (зачтено)	90 - 100	A (отлично)
4 (хорошо) (зачтено)	85 - 89	B (очень хорошо)
	75 - 84	C (хорошо)
	70 - 74	D (удовлетворительно)
3 (удовлетворительно) (зачтено)	65 - 69	
	60 - 64	E (посредственно)
2 (неудовлетворительно) (не зачтено)	Ниже 60 баллов	F (неудовлетворительно)

12. Учебно-методическое и информационное обеспечение дисциплины

12.1. Основная литература

1. Олифер, Виктор Григорьевич. Компьютерные сети: Принципы, технологии, протоколы : учебное пособие для вузов. - СПб. : Питер , 2006. - 960 с. (наличие в библиотеке ТУСУР - 92 экз.)

2. Основы информационной безопасности [Электронный ресурс]: Учебное пособие / А. М. Голиков - 2007. 201 с. - Режим доступа: https://edu.tusur.ru/publications/1024 (дата обращения: 10.07.2018).

12.2. Дополнительная литература

1. Защита информации в радиоэлектронных системах передачи информации [Электронный ресурс]: Курс лекций, компьютерные лабораторные работы, компьютерный практикум, задание на самостоятельную работу / А. М. Голиков - 2017. 913 с. - Режим доступа: https://edu.tusur.ru/publications/7072 (дата обращения: 10.07.2018).

12.3. Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Основы информационной безопасности [Электронный ресурс]: Учебное пособие для практических и семинарских занятий / А. М. Голиков - 2007. 154 с. - Режим доступа: https://edu.tusur.ru/publications/1017 (дата обращения: 10.07.2018).

2. Методические указания по лабораторным, самостоятельным работам и курсовой работе студентов по дисциплине "Сети и телекоммуникации". [Электронный ресурс]: - Режим доступа: http://kibevs.tusur.ru/sites/default/files/upload/work_progs/pga/seti.pdf (дата обращения: 10.07.2018).

12.3.2. Учебно-методические пособия для лиц с ограниченными возможностями здоровья и инвалидов

Учебно-методические материалы для самостоятельной и аудиторной работы обучающихся из числа лиц с ограниченными возможностями здоровья и инвалидов предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации.

Для лиц с нарушениями зрения:

- в форме электронного документа;
- в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:

- в форме электронного документа;
- в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

- в форме электронного документа;
- в печатной форме.

12.4. Профессиональные базы данных и информационные справочные системы

1. https://edu.tusur.ru – образовательный портал университета;
2. http://www.iqlib.ru – электронная интернет-библиотека;
3. http://www.biblioclub.ru – полнотестовая электронная библиотека;
4. http://www.elibrary.ru – научная электронная библиотека;
5. http://www.edu.ru – веб-сайт системы федеральных образовательных порталов.

13. Материально-техническое обеспечение дисциплины и требуемое программное обеспечение

13.1. Общие требования к материально-техническому и программному обеспечению дисциплины

13.1.1. Материально-техническое и программное обеспечение для лекционных занятий

Для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используется учебная аудитория с количеством посадочных мест не менее 22-24, оборудованная доской и стандартной учебной мебелью. Имеются демонстрационное оборудование и учебно-наглядные пособия, обеспечивающие тематические иллюстрации по лекционным разделам дисциплины.

13.1.2. Материально-техническое и программное обеспечение для практических занятий

Аудитория информатики, технологий и методов программирования

учебная аудитория для проведения занятий лекционного типа, учебная аудитория для проведения занятий практического типа, помещение для курсового проектирования (выполнения курсовых работ), помещение для самостоятельной работы

634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 408 ауд.

Описание имеющегося оборудования:

- Интерактивная доска IQBoard 78" с ПО ActivInspire;
- Проектор ViewSonic PJD5154 DLP;
- Компьютеры: DEPO Neos 235/ A8-7650K/ DDR3 4G/ 1Tb / мышь/ клавиатура/ монитор (10 шт.);
-Компьютер: DEPO Neos DF226/ i3-7100/ DDR4 8G/ Жесткий диск 500G/ мышь/ клавиатура/ монитор;
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

- Kaspersky endpoint security
- Microsoft Windows 10
- VirtualBox

13.1.3. Материально-техническое и программное обеспечение для самостоятельной работы

Для самостоятельной работы используются учебные аудитории (компьютерные классы), расположенные по адресам:

- 634050, Томская область, г. Томск, Ленина проспект, д. 40, 233 ауд.;
- 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 201 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 47, 126 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 74, 207 ауд.

Состав оборудования:

- учебная мебель;
- компьютеры класса не ниже ПЭВМ INTEL Celeron D336 2.8ГГц. - 5 шт.;
- компьютеры подключены к сети «Интернет» и обеспечивают доступ в электронную информационно-образовательную среду университета.

Перечень программного обеспечения:

- Microsoft Windows;
- OpenOffice;
- Kaspersky Endpoint Security 10 для Windows;
- 7-Zip;
- Google Chrome.

13.2. Материально-техническое обеспечение дисциплины для лиц с ограниченными возможностями здоровья и инвалидов

Освоение дисциплины лицами с ограниченными возможностями здоровья и инвалидами осуществляется с использованием средств обучения общего и специального назначения.

При занятиях с обучающимися **с нарушениями слуха** предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах, мобильной системы преподавания для обучающихся с инвалидностью, портативной индукционной системы. Учебная аудитория, в которой занимаются обучающиеся с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При занятиях с обучающимися **с нарушениями зрениями** предусмотрено использование в лекционных и учебных аудиториях возможности просмотра удаленных объектов (например, текста на доске или слайда на экране) при помощи видеоувеличителей для комфортного просмотра.

При занятиях с обучающимися **с нарушениями опорно-двигательного аппарата** используются альтернативные устройства ввода информации и другие технические средства приема/передачи учебной информации в доступных формах, мобильной системы обучения для людей с инвалидностью.

14. Оценочные материалы и методические рекомендации по организации изучения дисциплины

14.1. Содержание оценочных материалов и методические рекомендации

Для оценки степени сформированности и уровня освоения закрепленных за дисциплиной компетенций используются оценочные материалы в составе:

14.1.1. Тестовые задания

1. По масштабу компьютерные сети подразделяются на

a) звездообразные, кольцевые, шинные

b) одноранговые и сети "клиент-сервер"

c) проводные и беспроводные

d) локальные и глобальные

2. Какое из утверждений верно

a) Беспроводные сети являются более надёжным средством передачи сигналов, чем проводные

b) Для передачи сигналов в беспроводных сетях используются радиосигналы оптического

диапазона

c) Одномодовый волоконно-оптический кабель позволяет передавать сигналы на большие расстояния, чем многомодовый

d) Кабель типа «витая пара» позволяет передавать электрические сигналы на расстояния до 40 километров

3. Задачей какого уровня модели OSI является управление доступом к среде в сетях, построенных на основе разделяемой среды?

a) прикладного

b) сетевого

c) канального

d) физического

4. IP-адрес 192.168.0.5 относится к

a) Зарезервированному диапазону адресов для частных сетей, не маршрутизируемому в сети Интернет

b) Диапазону публичных адресов, маршрутизируемому в сети Интернет

c) Широковещательным адресам, которые используются для рассылки пакетов всем узлам локальной сети

d) Групповым адресам, используемым для маршрутизации

5. Маска подсети указывается вместе с ip-адресом и необходима для

a) определения MAC-адреса устройства-получателя

b) определения номера подсети, которой принадлежит ip-адрес

c) вычисления доменного имени сервера

d) вычисления адреса групповой рассылки в локальной сети

6. Переход на протокол IPv6 позволяет устранить следующую проблему

a) нехватка адресного пространства протокола IPv4

b) нехватка MAC-адресов устройств

c) медленное сопоставление доменного имени и IP-адреса

d) невозможность прямого преобразования MAC-адреса в доменное имя

7. К транспортному уровню модели OSI относятся протоколы:

a) IP, RIP, OSPF

b) SSL, TLS

c) SMTP, IMAP, POP3

d) UDP, TCP

8. Какое из утверждений верно

a) Протокол UDP гарантирует доставку данных получателю за счёт указания номера порта приложений отправителя и получателя

b) Протокол TCP является ненадёжным средством доставки данных, так как требует установления логического соединения

c) Протокол TCP гарантирует доставку данных за счёт установления логического соединения и подтверждения получения каждого сегмента данных

d) Протокол UDP является надёжным средством доставки данных, так как использует алгоритм скользящего окна

9. Что нужно сделать на DHCP сервере чтобы исключить выдачу определенного IP адреса из существующего диапазона?

a) создать диапазон IP адресов

b) создать параметр DHCP

c) создать область DHCP

d) создать исключение для IP адреса

10. Какое из утверждений является верным

a) Протокол http является безопасными протоколом передачи данных, т.к. позволяет использовать аутентификацию пользователя на веб-сервере

b) Протокол https является безопасным протоколом передачи данных, т.к. шифрует все данные с помощью протокола SSL/TLS

c) Протокол ftp шифрует данные на пароле пользователя

d) Протокол telnet позволяет безопасно подключаться и управлять удалённым сервером, так как его данные всегда проходят проверку межсетевой экран

11. Как называется объект Active Directory, который хранит информацию об учетных записях, общих ресурсах, подразделениях?

a) сетевой доступ

b) каталог

c) папка

d) домен

12. Компьютер, занимающийся обслуживанием сети, управлением передачей сообщений, и предоставляющий удаленный доступ к своим ресурсам, называется

a) хабом

b) сервером

c) рабочей станцией

d) хостом

13. Какое высказывание об угрозах безопасности информации в распределённых системах верно:

- Состав угроз безопасности информации в распределённых системах шире, т.к. к угрозам реализации атак на локальные компьютеры добавляются угрозы реализации атак с применение протоколов сетевого взаимодействия;

- Состав угроз безопасности информации в распределённых системах тот же что и в локальных, т.к. информация хранится и обрабатывается на компьютерах, а не в сетевом оборудовании;

- Количество угроз безопасности информации в распределённых системах ниже, чем в локальных, т.к. в современных компьютерных сетях применяются безопасные протоколы сетевого взаимодействия;

- Количество угроз безопасности информации в распределённых системах больше по сравнению с локальными, т.к. пользователи распределённой системы работают с ресурсами сети Интернет.

14. Межсетевое экранирование в распределённых информационных системах позволяет:

- осуществлять фильтрацию сетевых пакетов в соответствии с правилами политики безопасности информационной системы;

- скрыть код информационной системы от изучения программами-декомпиляторами;

- осуществлять блокирование сетевых пакетов, не прошедших процедуру аутентификации;

- скрыть от внутренних злоумышленников структуру и состав защищенной распределённой информационной системы.

15. Какие основные разновидности VPN-соединений применяются в распределённых системах?

- Host-to-site и Site-to-site;

- Host-to-host и межсерверные виртуальные каналы;

- Site-to-host и Site-to-system;

- шифрованные и не шифрованные.

16. Пакетные фильтры принимают решение по пропуске/блокировании пакета на основании:

- данных, расположенных в заголовке ip-пакета;

- данных, расположенных в сегменте протокола TCP;

- направления пересылки данных;

- наличия запрещённых слов и сайтов в запросе HTTP.

17. Системы обнаружения вторжений способны:

- выявлять атаки на ресурсы сети или операционной системы в реальном масштабе времени;

- сканировать сетевые ресурсы и сообщать о возможных методах проникновения нарушителя в информационную систему;

- анализировать записи безопасности за указанный период и сообщать о произошедших ранее атаках;

- отправлять администратру безопасности о выходе обноалений и исправления операцион-

ных систем и прикладного программного обеспечения для скорейшего устранения уязвимостей.

18. Сканеры безопасности могут выявлять уязвимости:

- в сетевых протоколах и настройказ операционных систем;
- в программном коде подозрительных приложений;
- в сообщениях электроной почты, поступающих в корпоративный ящик электронной почты;
- в документах, загружаемых по протоколу HTTP.

19. Межсетевые экраны нового поколения (NGFW) отличаютсч от традиционных межсетевых экранов:

- интерграцией различных механизмов защииты в одном устройстве;
- повышенной производительностью;
- поддержкой оптических сетевых интерфейсов;
- наличием лицензии на блок антивирусной защиты.

20. Защита виртуальной инфраструктуры может обеспечиваться:

- специальными программными средствами защиты, устанавливаемыми как на гипервозирах, так и на границе сети управления виртуальной инфраструктурой.
- штатными средства гипервизоров и виртуальных машин;
- традиционными межсетевыми экранами и средствами обнаружения вторжений, устанавливаемыми на границе виртуальной сети;
- дополнительными средствами защиты информации, устанавливаемыми на рабочей станции администратора информационной безопасности.

14.1.2. Вопросы для подготовки к практическим занятиям, семинарам

Настройка подключения хоста к локальной сети. Базовые службы локальных и шлобальных сетей.

Анализ угроз безопасности информации и их источников. Планирование структуры системы защиты информации

Анализ угроз безопасности информации в системе. Составление модели угроз.

Планирование структуры системы защиты информации в компьютерной сети. Обоснование выбоора методов и средств защиты информации.

Защита информации от несанкционированного доступа штатными и дополнительными средствами операционных систем

Разграничение доступа к сетевым устройствам, хостам и информационным ресурсам локальной сети

DLP-системы.

Межсетевые экраны

Системы обнаружения и предотвращения вторжений.

Технология VPN.

Сканеры безопасности

Антивирусная защита

Защита информации в виртуальной инфраструктуре.

Защита персональных данных в соответствии с требованиями нормативных документов

Защита конфиденциальной информации в соответствии с требованиями номативных документов

14.1.3. Темы опросов на занятиях

Предмет, цель и содержание дисциплины. Место и роль вычислительных сетей в современном мире. Общие представления о вычислительной сети. Вычислительные сети и распределенные системы.

Принципы многоуровневой организации локальных и глобальных сетей ЭВМ. Модель OSI. Уровни модели OSI. Стандартные стеки коммуникационных протоколов.

Основное коммуникационное оборудование (сетевые адаптеры и концентраторы, мосты и коммутаторы, маршрутизаторы).

Технология Ethernet (IEEE802.3).

Построение сетей на основе сетевого уровня.

Реализация межсетевого взаимодействия средствами TCP/IP. Протоколы IP, UDP, TCP. Про-

токолы прикладного уровня.

Основные понятия в области информационной безопасности. Конфиденциальность, целостность, доступность информации (информационного ресурса).

Понятия угроза, уязвимость, атака.

Классификация угроз. Источники угроз.

Классификация уязвимостей. Источники уязвимостей. База уязвимостей CVE.

Классификация атак. Типовой сценарий реализации атак.

Специфические угрозы при подключении узлов к вычислительной сети.

Уязвимости протоколов сетевого взаимодействия и распределенных информационных систем.

Типовые атаки на локальные и распределенные вычислительные сети.

Базовые механизмы защиты информации в локальных и глобальных сетях.

Разграничение доступа к сетевым ресурсам. Межсетевое экранирование. Антивирусная защита. Виртуальные честные сети (VPN).

Дополнительные механизмы защиты в локальных и глобальных

Примеры реализации сетевых атак.

Типовой сценарий реализации сетевых атак.

Защита от несанкционированного доступа к узлам и информационным ресурсам в локальных сетях.

Ограничение доступа к сетевым установсикам средствами операционной системы хоста.

Предотвращение утечки информации в результате действий внутренних злоумышленников.

Защита периметра информационной системы межсетевыми экранами. Понятие демилитаризованной зоны.

Атнивирусная защита компьютерных сете.

Обнаружение и предоьвращение вторжений. Классификация систем обнаружения вторжени.

Применение технологии виртуальных частных сетей для защиты каналов связи компьютерных сетей. Основные компоненты VPN.

Сканирование ресурсов и узолов сети на наличие уязвимостей и соответствие требованиям нормативных документов по защите информации.

Современные технологии защиты информации в компьютерных сетях. Технология NGFW. Защита информации в виртуальной инфраструктуре.

Требования нормативных документов по защите персональных данных при обработке и перевысле в локальных и глобальных сетях.

Требования нормативных документов по защите конфиденциальной информации.

Управление информационной безопасностью компьютерынх сетей.

14.1.4. Вопросы дифференцированного зачета

1. Основные проблемы построения сетей
2. Требования к сетям
3. Классификация сетей
4. Проблемы стандартизации
5. Стек протоколов TCP/IP как средство построения больших сетей
6. Адресация в IP-сетях
7. Протокол межсетевого взаимодействия IP
8. Протокол доставки пользовательских дейтаграмм UDP
9. Протокол надежной доставки сообщений TCP
10. Протокол обмена управляющими сообщениями ICMP
11. Протоколы обмена маршрутной информацией стека TCP/IP
12. Протоколы прикладного уровня
13. Основные понятия информационной безопасности
14. Угрозы безопасности вычислительных сетей
15. Основные средства обеспечения сетевой безопасности
16. Безопасность физического и канального уровней модели OSI.
17. Сетевые анализаторы и «снифферы»
18. Безопасность сетевого уровня модели OSI.

19. Межсетевые и персональные экраны (firewall)
20. Критерии оценки межсетевых экранов
21. Построение защищенных сетей с помощью технологии VPN. Типы систем VPN
22. Определение различий между типами VPN
23. Безопасность транспортного уровня модели OSI.
24. Меры защиты транспортного уровня. Протоколы SSL, SSH
25. Проблемы безопасности протоколов прикладного уровня
26. Модель безопасности ОС Windows
27. Модель безопасности СУБД Microsoft SQL Server

14.2. Требования к оценочным материалам для лиц с ограниченными возможностями здоровья и инвалидов

Для лиц с ограниченными возможностями здоровья и инвалидов предусмотрены дополнительные оценочные материалы, перечень которых указан в таблице 14.

Таблица 14 – Дополнительные материалы оценивания для лиц с ограниченными возможностями здоровья и инвалидов

Категории обучающихся	Виды дополнительных оценочных материалов	Формы контроля и оценки результатов обучения
С нарушениями слуха	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы	Преимущественно письменная проверка
С нарушениями зрения	Собеседование по вопросам к зачету, опрос по терминам	Преимущественно устная проверка (индивидуально)
С нарушениями опорно-двигательного аппарата	Решение дистанционных тестов, контрольные работы, письменные самостоятельные работы, вопросы к зачету	Преимущественно дистанционными методами
С ограничениями по общемедицинским показаниям	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы, устные ответы	Преимущественно проверка методами исходя из состояния обучающегося на момент проверки

14.3. Методические рекомендации по оценочным материалам для лиц с ограниченными возможностями здоровья и инвалидов

Для лиц с ограниченными возможностями здоровья и инвалидов предусматривается доступная форма предоставления заданий оценочных средств, а именно:

- в печатной форме;
- в печатной форме с увеличенным шрифтом;
- в форме электронного документа;
- методом чтения ассистентом задания вслух;
- предоставление задания с использованием сурдоперевода.

Лицам с ограниченными возможностями здоровья и инвалидам увеличивается время на подготовку ответов на контрольные вопросы. Для таких обучающихся предусматривается доступная форма предоставления ответов на задания, а именно:

- письменно на бумаге;
- набор ответов на компьютере;
- набор ответов с использованием услуг ассистента;
- представление ответов устно.

Процедура оценивания результатов обучения лиц с ограниченными возможностями здоровья и инвалидов по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

- в форме электронного документа;
- в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:

- в форме электронного документа;
- в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

- в форме электронного документа;
- в печатной форме.

При необходимости для лиц с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения может проводиться в несколько этапов.