МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

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

УТВЕРЖДАЮ
Проректор по учебной работе
_____ П. Е. Троян
«___» _____ 20__ г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Безопасность сетей ЭВМ

Уровень образования: **высшее образование - специалитет**
Направление подготовки (специальность): **10.05.03 Информационная безопасность автоматизированных систем**
Направленность (профиль): **Информационная безопасность автоматизированных банковских систем**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**
Курс: **3**
Семестр: **5, 6**
Учебный план набора 2016 года

Распределение рабочего времени

№	Виды учебной деятельности	5 семестр	6 семестр	Всего	Единицы
1	Лекции	18	28	46	часов
2	Практические занятия		18	18	часов
3	Лабораторные работы	36	44	80	часов
4	Всего аудиторных занятий	54	90	144	часов
5	Из них в интерактивной форме	16	24	40	часов
6	Самостоятельная работа	18	54	72	часов
7	Всего (без экзамена)	72	144	216	часов
8	Подготовка и сдача экзамена		36	36	часов
9	Общая трудоемкость	72	180	252	часов
		2.0	5.0	7.0	З.Е

Зачет: 5 семестр
Экзамен: 6 семестр

Согласована на портале № 15401

Рассмотрена и одобрена на заседании кафедры
протокол № 2 от «15» 2 2017 г.

Томск 2017

Согласована на портале № 15401

ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 10.05.03 Информационная безопасность автоматизированных систем, утвержденного 2016-12-01 года, рассмотрена и утверждена на заседании кафедры «___» _____ 20__ года, протокол №_____.

Разработчики:

ассистент каф. КИБЭВС _____ Новохрестов А. К.

Заведующий обеспечивающей каф. КИБЭВС _____ Шелупанов А. А.

Рабочая программа согласована с факультетом, профилирующей и выпускающей кафедрами направления подготовки (специальности).

Декан ФБ _____ Давыдова Е. М.

Заведующий выпускающей каф. КИБЭВС _____ Шелупанов А. А.

Эксперты:

доцент каф. КИБЭВС _____ Конев А. А.

Согласована на портале № 15401

1. Цели и задачи дисциплины

1.1. Цели дисциплины

Обучить студентов основам построения и эксплуатации вычислительных сетей, принципам и методам защиты информации в компьютерных сетях, навыкам комплексного проектирования, построения, обслуживания и анализа защищенных вычислительных сетей.

1.2. Задачи дисциплины

- Дать основы:
- – архитектуры вычислительных сетей;
- – программно-аппаратных и технических средств создания сетей;
- – принципов построения сетей и управления ими;
- – использования программных и аппаратных технологий защиты сетей;
- – методологии проектирования, развертывания и сопровождения безопасных сетей;
- – обследования и анализа защищенных вычислительных сетей.
-

2. Место дисциплины в структуре ОПОП

Дисциплина «Безопасность сетей ЭВМ» (Б1.Б.9) относится к блоку 1 (базовая часть).

Предшествующими дисциплинами, формирующими начальные знания, являются следующие дисциплины: Информатика, Основы информационной безопасности.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- ПК-3 способностью проводить анализ защищенности автоматизированных систем;
- ПК-14 способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации;
- ПК-17 способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации;
- ПК-26 способностью администрировать подсистему информационной безопасности автоматизированной системы;

В результате изучения дисциплины студент должен:

- **знать** средства и методы хранения и передачи информации; эталонную модель взаимодействия открытых систем; основные стандарты в области инфокоммуникационных систем и технологий; основные нормативно правовые акты и нормативные методические документы в области инфокоммуникационных систем; 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 в соответствии с требованиями нормативно правовых актов и нормативных методических документов.
- **владеть** навыками конфигурирования локальных сетей, навыками реализации сетевых протоколов с помощью программных средств; навыками настройки межсетевых экранов; навыками применения нормативно правовых актов и нормативных методических документов в области инфокоммуникационных систем; методикой анализа сетевого трафика; методикой анализа результатов работы средств обнаружения вторжений.

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 7.0 зачетных единицы и представлена в таблице 4.1.

Согласована на портале № 15401

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры	
		5 семестр	6 семестр
Аудиторные занятия (всего)	144	54	90
Лекции	46	18	28
Практические занятия	18		18
Лабораторные работы	80	36	44
Из них в интерактивной форме	40	16	24
Самостоятельная работа (всего)	72	18	54
Оформление отчетов по лабораторным работам	31	9	22
Проработка лекционного материала	35	9	26
Подготовка к практическим занятиям, семинарам	6		6
Всего (без экзамена)	216	72	144
Подготовка и сдача экзамена	36		36
Общая трудоемкость ч	252	72	180
Зачетные Единицы	7.0	2.0	5.0

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	Лекции	Практические занятия	Лабораторные работы	Самостоятельная работа	Всего часов (без экзамена)	Формируемые компетенции
5 семестр						
1 Основные понятия информационных сетей	4	0	8	4	16	ПК-26, ПК-3
2 Основы построения современных локальных сетей	4	0	8	4	16	ПК-17, ПК-3
3 Сетевые операционные системы	2	0	8	3	13	ПК-26, ПК-3
4 Средства реализации межсетевого взаимодействия	6	0	12	6	24	ПК-26, ПК-3
5 Перспективные направления развития и проблемы информационных сетей	2	0	0	1	3	ПК-3
Итого за семестр	18	0	36	18	72	
6 семестр						

Согласована на портале № 15401

6 Основные понятия информационной безопасности	4	0	0	4	8	ПК-17, ПК-3
7 Технологии обеспечения безопасности в локальных сетях	8	18	12	26	64	ПК-14, ПК-17, ПК-26, ПК-3
8 Обеспечение безопасности сетей на базе сетевых операционных систем	6	0	0	4	10	ПК-14, ПК-26, ПК-3
9 Обеспечение безопасности межсетевого взаимодействия	6	0	32	16	54	ПК-14, ПК-17, ПК-26, ПК-3
10 Правовые основы защиты информации в компьютерных сетях. Защищенный документооборот	4	0	0	4	8	ПК-14, ПК-3
Итого за семестр	28	18	44	54	144	
Итого	46	18	80	72	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
5 семестр			
1 Основные понятия информационных сетей	История развития сетей ЭВМ. Место и роль вычислительных сетей в современном мире. Основные понятия и терминология. Общие представления о вычислительной сети. Общее понятие об иерархической структуре протоколов. Принципы многоуровневой организации локальных и глобальных сетей ЭВМ. Модель OSI. Стандартные стеки коммуникационных протоколов.	2	ПК-3
	Стандартизация в сетях. Классификация вычислительных сетей. Требования, предъявляемые к современным вычислительным сетям. Методы и технологии проектирования средств телекоммуникаций. Структуризации сети. Физическая и логическая топологии сетей. Основное коммуникационное оборудование	2	
	Итого	4	
2 Основы построения современных локальных сетей	Каналы связи. Характеристики каналов связи. Логическое кодирование. Асинхронная и синхронная передачи.	2	ПК-17, ПК-3

Согласована на портале № 15401

	Иерархия в кабельной системе. Структурированная кабельная система.		
	Конфигурации локальных вычислительных сетей и методы доступа в них. Структура и функции локальных сетей. Содержание стандарта IEEE 802. Базовые технологии локальных сетей. IEEE 802.2 Ethernet. Оборудование локальных сетей.	2	
	Итого	4	
3 Сетевые операционные системы	Программные средства телекоммуникации. Структура программного обеспечения локальной сети. Классификация программного обеспечения локальных сетей. Принципы построения сетевого программного обеспечения и сетевых операционных систем. Классификация серверов. Проектирование сетей ЭВМ по принципу «клиент-сервер».	2	ПК-3
	Итого	2	
4 Средства реализации межсетевого взаимодействия	Сетевой уровень передачи данных. IP-адресация. Реализация межсетевого взаимодействия средствами TCP/IP. Порядок распределения IP-адресов. Отображение IP-адресов на локальные адреса. ARP протокол.	2	ПК-3
	Принципы маршрутизации в IP-сетях. Протоколы маршрутизации. Понятие домена. Доменная адресация в IP-сетях. DNS протокол.	2	
	Протокол IPv6. Протоколы транспортного уровня TCP и UDP.	2	
	Итого	6	
5 Перспективные направления развития и проблемы информационных сетей	Современные тенденции развития телекоммуникационных систем. Интеграция различных типов сетей и сетевых служб. Виртуализация информационных систем. Облачные вычисления.	2	ПК-3
	Итого	2	
Итого за семестр		18	
6 семестр			
6 Основные понятия информационной безопасности	Обеспечение безопасности телекоммуникационных связей и административный контроль. Основные понятия и терминология.	2	ПК-17, ПК-3

Согласована на портале № 15401

	Типовые угрозы сетевой безопасности. Основы классификации сетевых угроз и атак. Влияние человеческого фактора на сетевую безопасность.	2	
	Итого	4	
7 Технологии обеспечения безопасности в локальных сетях	Защита топологии сети. Виртуальные локальные сети. Дополнительные функции коммутаторов. Персональные экраны. Абонентское шифрование.	2	ПК-14, ПК-17, ПК-26, ПК-3
	Защита сетевого трафика и компонентов сети. Защита компонентов сети от НСД. Безопасность ресурсов сети. Средства идентификации и аутентификации, методы разделения ресурсов и технологии разграничения доступа.	2	
	Средства повышения надежности функционирования сетей. Защита от сбоев электропитания, аппаратного и программного обеспечения. Контроль и распределение нагрузки на вычислительную сеть.	2	
	Регламентирующие документы в области безопасности вычислительных сетей. Стандарты безопасности вычислительных сетей и их компонентов. Правовые основы защиты информации в сетях.	2	
	Итого	8	
8 Обеспечение безопасности сетей на базе сетевых операционных систем	Сетевые операционные системы Windows, Unix/Linux. Основные протоколы, службы, функционирование, средства обеспечения безопасности, средства управления и контроля.	2	ПК-14, ПК-26, ПК-3
	Политика безопасности: Понятие политики безопасности. Типовые элементы политики безопасности. Построение, реализация, поддержание и модификация политики безопасности.Критерии оценки безопасности сетевых ОС. Основные критерии анализа сетевой безопасности. Общая процедура анализа.	4	
	Итого	6	
9 Обеспечение безопасности межсетевого взаимодействия	Основные механизмы обеспечения безопасности и управления распределенными ресурсами. Обеспечение надежности	2	ПК-14, ПК-17, ПК-26, ПК-3

Согласована на портале № 15401

	инфраструктуры Интернет.		
	Защита каналов связи в Интернет. Виды используемых в Интернет каналов связи. Использование межсетевых экранов. Виртуальные частные сети.	2	
	Уязвимости и защита базовых протоколов и служб: Протоколы маршрутизации. Семейство TCP/IP. Службы поиска. Безопасность WWW и электронной почты.	2	
	Итого	6	
10 Правовые основы защиты информации в компьютерных сетях. Защищенный документооборот	Системы обнаружения и противодействия вторжениям. Классификация и принципы функционирования систем обнаружения вторжений. Сканеры безопасности.	2	ПК-14, ПК-3
	Классы сканеров безопасности и особенности применения. Защита от вирусов.Защита электронного документооборота.	2	
	Итого	4	
Итого за семестр		28	
Итого		46	

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	8	9	10
Предшествующие дисциплины										
1 Информатика	+		+							
2 Основы информационной безопасности						+				

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 и видов занятий, формируемых при изучении дисциплины

	Виды занятий	Формы контроля

Согласована на портале № 15401

Компетенции	Лекции	Практические занятия	Лабораторные работы	Самостоятельная работа	
ПК-3	+	+	+	+	Защита отчета, Отчет по лабораторной работе, Опрос на занятиях
ПК-14	+	+	+	+	Защита отчета, Отчет по лабораторной работе, Опрос на занятиях
ПК-17	+		+	+	Защита отчета, Отчет по лабораторной работе, Опрос на занятиях
ПК-26	+	+	+	+	Защита отчета, Отчет по лабораторной работе, Опрос на занятиях

6. Интерактивные методы и формы организации обучения

Технологии интерактивного обучения при разных формах занятий в часах приведены в таблице 6.1

Таблица 6.1 – Технологии интерактивного обучения при разных формах занятий в часах

Методы	Интерактивные лабораторные занятия	Интерактивные лекции	Интерактивные практические занятия	Всего
5 семестр				
IT-методы	10			10
Презентации с использованием слайдов с обсуждением		6		6
Итого за семестр:	10	6	0	16
6 семестр				
IT-методы	12			12
Презентации с использованием слайдов с обсуждением		8		8
Исследовательский метод			4	4
Итого за семестр:	12	8	4	24
Итого	22	14	4	40

7. Лабораторные работы

Наименование лабораторных работ приведено в таблице 7.1.

Согласована на портале № 15401

Таблица 7. 1 – Наименование лабораторных работ

Названия разделов	Наименование лабораторных работ	Трудоемкость, ч	Формируемые компетенции
5 семестр			
1 Основные понятия информационных сетей	Моделирование сетевых устройств и протоколов в локальных сетях	4	ПК-26, ПК-3
	Моделирование виртуальных локальных сетей (VLAN) с разграничением доступа к сетевым ресурсам	4	
	Итого	8	
2 Основы построения современных локальных сетей	Настройка подключения узла к сети. Автоматическая динамическая и статическая настройки сетевого подключения.	4	ПК-3
	Стек протоколов TCP/IP. Прикладные протоколы сети Интернет.	4	
	Итого	8	
3 Сетевые операционные системы	Сети Microsoft Windows. Управление сетевыми ресурсами в одноранговой сети.	4	ПК-26, ПК-3
	Сети Microsoft Windows. Active Directory. Управление сетевыми ресурсами корпоративной сети. Групповые политики.	4	
	Итого	8	
4 Средства реализации межсетевого взаимодействия	Моделирование базовых служб и протоколов маршрутизации в глобальных сетях.	4	ПК-26, ПК-3
	Базовые службы сети Интернет. DHCP. DNS. Протоколы маршрутизации.	4	
	Прикладные службы сети Интернет. Настройка Web-, FTP-серверов и сервера электронной почты.	4	
	Итого	12	
Итого за семестр		36	
6 семестр			
7 Технологии обеспечения безопасности в локальных сетях	Разграничение доступа к локальным и сетевым ресурсам. Дискреционная и мандатная модели управления доступом.	4	ПК-14, ПК-17, ПК-26, ПК-3
	Инструменты для исследования сети (сниферы)	4	

Согласована на портале № 15401

	Инструменты для исследования сети (сканеры безопасности)	4	
	Итого	12	
9 Обеспечение безопасности межсетевого взаимодействия	Межсетевые экраны	4	ПК-14, ПК-17, ПК-26, ПК-3
	Антивирусная защита	4	
	Виртуальные частные сети	8	
	Системы обнаружения и предотвращения вторжений	4	
	DLP-системы	8	
	Безопасность прикладных протоколов	4	
	Итого	32	
Итого за семестр		44	
Итого		80	

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
6 семестр			
7 Технологии обеспечения безопасности в локальных сетях	Построение структуры информационной сети, описание характера связей между элементами и информационных потоков.	4	ПК-14, ПК-26, ПК-3
	Проработка модели угроз и модели нарушителя компьютерной сети.	4	
	Проработка структуры системы защиты информации, состава средств защиты. Изучение способов установки и основных параметров конфигурации средств защиты информации	6	
	Подготовка документов по системе защиты информации в информационной системе.	4	
	Итого	18	
Итого за семестр		18	
Итого		18	

9. Самостоятельная работа

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

Согласована на портале № 15401

Таблица 9.1 - Виды самостоятельной работы, трудоемкость и формируемые компетенции

Названия разделов	Виды самостоятельной работы	Трудоемкость, ч	Формируемые компетенции	Формы контроля
5 семестр				
1 Основные понятия информационных сетей	Проработка лекционного материала	2	ПК-26, ПК-3	Опрос на занятиях, Отчет по лабораторной работе
	Оформление отчетов по лабораторным работам	2		
	Итого	4		
2 Основы построения современных локальных сетей	Проработка лекционного материала	2	ПК-17, ПК-3	Опрос на занятиях, Отчет по лабораторной работе
	Оформление отчетов по лабораторным работам	2		
	Итого	4		
3 Сетевые операционные системы	Проработка лекционного материала	1	ПК-26, ПК-3	Опрос на занятиях, Отчет по лабораторной работе
	Оформление отчетов по лабораторным работам	2		
	Итого	3		
4 Средства реализации межсетевого взаимодействия	Проработка лекционного материала	3	ПК-26, ПК-3	Опрос на занятиях, Отчет по лабораторной работе
	Оформление отчетов по лабораторным работам	3		
	Итого	6		
5 Перспективные направления развития и проблемы информационных сетей	Проработка лекционного материала	1	ПК-3	Опрос на занятиях
	Итого	1		
Итого за семестр		18		
6 семестр				
6 Основные понятия информационной безопасности	Проработка лекционного материала	4	ПК-17, ПК-3	Опрос на занятиях
	Итого	4		
7 Технологии обеспечения безопасности в локальных сетях	Подготовка к практическим занятиям, семинарам	6	ПК-14, ПК-17, ПК-26, ПК-3	Защита отчета, Опрос на занятиях, Отчет по лабораторной работе
	Проработка лекционного материала	8		
	Оформление отчетов по лабораторным работам	12		
	Итого	26		

Согласована на портале № 15401

8 Обеспечение безопасности сетей на базе сетевых операционных систем	Проработка лекционного материала	4	ПК-14, ПК-26, ПК-3	Опрос на занятиях
	Итого	4		
9 Обеспечение безопасности межсетевого взаимодействия	Проработка лекционного материала	6	ПК-14, ПК-17, ПК-26, ПК-3	Опрос на занятиях, Отчет по лабораторной работе
	Оформление отчетов по лабораторным работам	10		
	Итого	16		
10 Правовые основы защиты информации в компьютерных сетях. Защищенный документооборот	Проработка лекционного материала	4	ПК-14, ПК-3	Опрос на занятиях
	Итого	4		
Итого за семестр		54		
	Подготовка и сдача экзамена	36		Экзамен
Итого		108		

10. Курсовая работа (проект)

Не предусмотрено РУП

11. Рейтинговая система для оценки успеваемости студентов

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
5 семестр				
Опрос на занятиях	3	4	3	10
Отчет по лабораторной работе	30	30	30	90
Итого максимум за период	33	34	33	100
Нарастающим итогом	33	67	100	100
6 семестр				
Защита отчета	10	10		20
Опрос на занятиях	3	4	3	10
Отчет по лабораторной работе		20	20	40
Итого максимум за период	13	34	23	70
Экзамен				30
Нарастающим итогом	13	47	70	100

Согласована на портале № 15401

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. Компьютерные сети: Принципы, технологии, протоколы [Текст] : учебник для вузов / В. Г. Олифер, Н. А. Олифер. - 4-е изд. - СПб. : ПИТЕР, 2013. - 944 с. : ил., табл. - (Учебник для вузов. Стандарт третьего поколения). - Алф. указ.: с. 918-943. - ISBN 978-5-496-00004-8 : 470.69 р. (наличие в библиотеке ТУСУР - 20 экз.)

2. Компьютерные сети [Текст] : научное издание / Э. Таненбаум, Д. Уэзеролл. - 5-е изд. - СПб. : ПИТЕР, 2013. - 960 с. : ил., табл. - (КЛАССИКА COMPUTER SCIENCE). - Пер. с англ. - Алф. указ.: с. 947-955. - ISBN 978-5-4461-0068-2 : 1244.32 р. (наличие в библиотеке ТУСУР - 15 экз.)

12.2. Дополнительная литература

1. Сетевые операционные системы : Учебное пособие для вузов / В. Г. Олифер, Н. А. Олифер. - СПб. : Питер, 2007. - 538[6] с. : ил. - (Учебник для вузов). - Библиогр.: с. 525-526. - Алф. указ.: с. 527-538. - ISBN 5-272-00120-6 : 145.20 р. (наличие в библиотеке ТУСУР - 10 экз.)

12.3 Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Безопасность сетей ЭВМ: Методические указания для лабораторных и практических работ / Новохрестов А. К., Праскурин Г.А., 2014. – 99 с. [Электронный ресурс] [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/work_progs/nak/BSEVM_lab_pract.pdf

2. Безопасность сетей ЭВМ: Методические указания для самостоятельной работы студента / Новохрестов А.К., Праскурин Г.А., 2014. – 4 с. [Электронный ресурс] [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/work_progs/nak/BSEVM_sam.pdf

Согласована на портале № 15401

12.3.2 Учебно-методические пособия для лиц с ограниченными возможностями здоровья

Учебно-методические материалы для самостоятельной и аудиторной работы обучающихся из числа 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. Базы данных, информационно-справочные, поисковые системы и требуемое программное обеспечение

1. http://www.lib.tusur.ru – библиотека университета;
2. http://www.elibrary.ru – научная электронная библиотека;
3. http://www.edu.ru – веб-сайт системы федеральных образовательных порталов.
4.
5. Программное обеспечение:
6. операционные системы семейства Windows;
7. средство защиты информации "Блокхост-сеть К";
8. система обнаружения вторжений "Snort";
9. средство моделирования сетей Cisco Packet Tracer;
10. DLP-система "Контур информационной безопасности SearchInform";
11. дистрибутив Kali Linux;
12. система анализа защищенности сети "MaxPatrol".

13. Материально-техническое обеспечение дисциплины

13.1. Общие требования к материально-техническому обеспечению дисциплины

13.1.1. Материально-техническое обеспечение для лекционных занятий

Для проведения лекционных занятий используется учебно-исследовательская вычислительная лаборатория, расположенная по адресу 634045, Томская область, г. Томск, Красноармейская улица, д. 146, 3 этаж, ауд. 310. Состав оборудования: Учебная мебель; Экран раздвижной - 1 шт.; Доска магнитно-маркерная - 1 шт.; Мультимедийный проектор ViewSonic PJD5151 – 1 шт.; Компьютер лекционный acer travelmate 2300; Используется лицензионное программное обеспечение, пакеты версией не ниже: Microsoft Windows XP SP2, Microsoft Powerpoint Viewer; Имеется помещение для хранения и профилактического обслуживания учебного оборудования.

13.1.2. Материально-техническое обеспечение для практических занятий

Для проведения практических занятий используется учебно-исследовательская вычислительная лаборатория, расположенная по адресу 634045, Томская область, г. Томск, Красноармейская улица, д. 146, 8 этаж, ауд. 804. Состав оборудования: Учебная мебель;– 1 шт.; Доска магнитно-маркерная - 1 шт.; Компьютеры класса не ниже CPU AMD A4-6300/DDR-III DIMM 4Gb x2/ HDD 250 Gb SATA-II 300 Seagate Pipeline HD.2 . с широкополосным доступом в Internet, – 10 шт.; Используется лицензионное программное обеспечение, пакеты версией не ниже: Microsoft Windows 8.1 Professional; Visual Studio 2012; Oracle VM VirtualBox; VMware Player. Имеется помещение для хранения и профилактического обслуживания учебного оборудования. Экран раздвижной - 1 шт.; Мультимедийный проектор ViewSonic PJD5151

13.1.3. Материально-техническое обеспечение для лабораторных работ

Для проведения лабораторных занятий используется учебно-исследовательская вычислительная лаборатория, расположенная по адресу 634045, Томская область, г. Томск,

Согласована на портале № 15401

Красноармейская улица, д. 146, 8 этаж, ауд. 804. Состав оборудования: Учебная мебель;– 1 шт.; Доска магнитно-маркерная - 1 шт.; Компьютеры класса не ниже CPU AMD A4-6300/DDR-III DIMM 4Gb x2/ HDD 250 Gb SATA-II 300 Seagate Pipeline HD.2 . с широкополосным доступом в Internet, – 10 шт.; Используется лицензионное программное обеспечение, пакеты версией не ниже: Microsoft Windows 8.1 Professional; Visual Studio 2012; Oracle VM VirtualBox; VMware Player. Имеется помещение для хранения и профилактического обслуживания учебного оборудования. Экран раздвижной - 1 шт.; Мультимедийный проектор ViewSonic PJD5151

13.1.4. Материально-техническое обеспечение для самостоятельной работы

Для самостоятельной работы используется учебная аудитория (компьютерный класс), расположенная по адресу 634034, г. Томск, ул. Красноармейская, 146, 2 этаж, ауд. 204. Состав оборудования: учебная мебель; компьютеры класса не ниже ПЭВМ INTEL Ce1егоп D336 2.8ГГц. - 7 шт.; компьютеры подключены к сети ИНТЕРНЕТ и обеспечивают доступ в электронную информационно-образовательную среду университета.

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

Освоение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения общего и специального назначения.

При обучении студентов **с нарушениями слуха** предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах для студентов с нарушениями слуха, мобильной системы обучения для студентов с инвалидностью, портативной индукционной системы. Учебная аудитория, в которой обучаются студенты с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При обучении студентов **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 удаленного просмотра.

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

14. Фонд оценочных средств

14.1. Основные требования к фонду оценочных средств и методические рекомендации

Фонд оценочных средств и типовые контрольные задания, используемые для оценки сформированности и освоения закрепленных за дисциплиной компетенций при проведении текущей, промежуточной аттестации по дисциплине приведен в приложении к рабочей программе.

14.2 Требования к фонду оценочных средств для лиц с ограниченными возможностями здоровья

Для студентов с инвалидностью предусмотрены дополнительные оценочные средства, перечень которых указан в таблице.

Таблица 14 – Дополнительные средства оценивания для студентов с инвалидностью

Категории студентов	Виды дополнительных оценочных средств	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-	Решение дистанционных тестов, контрольные работы, письменные	Преимущественно дистанционными методами

Согласована на портале № 15401

двигательного аппарата	самостоятельные работы, вопросы к зачету	
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 средствам для лиц с ограниченными возможностями здоровья

Для студентов с ОВЗ 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.

Студентам с инвалидностью увеличивается время на подготовку ответов на контрольные вопросы. Для таких студентов 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 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 обучающихся с инвалидностью процедура оценивания результатов обучения может проводиться в несколько этапов.

Согласована на портале № 15401

Приложение 1

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

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

УТВЕРЖДАЮ
Проректор по учебной работе
_____ П. Е. Троян
«___» _____ 20__ г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

Безопасность сетей ЭВМ

Уровень образования: **высшее образование - специалитет**
Направление подготовки (специальность): **10.05.03 Информационная безопасность автоматизированных систем**
Направленность (профиль): **Информационная безопасность автоматизированных банковских систем**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**
Курс: **3**
Семестр: **5, 6**

Учебный план набора 2016 года

Разработчики:

- ассистент каф. КИБЭВС Новохрестов А. К.

Зачет: 5 семестр
Экзамен: 6 семестр

Томск 2017

Согласована на портале № 15401

1. Введение

Фонд оценочных средств (ФОС) является приложением к рабочей программе дисциплины (практики) и представляет собой совокупность контрольно-измерительных материалов (типовые задачи (задания), контрольные работы, тесты и др.) и методов их использования, предназначенных для измерения уровня достижения студентом установленных результатов обучения.

ФОС по дисциплине (практике) используется при проведении текущего контроля успеваемости и промежуточной аттестации студентов.

Перечень закрепленных за дисциплиной (практикой) компетенций приведен в таблице 1.

Таблица 1 – Перечень закрепленных за дисциплиной компетенций

Код	Формулировка компетенции	Этапы формирования компетенций
ПК-26	способностью администрировать подсистему информационной безопасности автоматизированной системы	Должен знать средства и методы хранения и передачи информации; эталонную модель взаимодействия открытых систем; основные стандарты в области инфокоммуникационных систем и технологий; основные нормативно правовые акты и нормативные методические документы в области инфокоммуникационных систем; 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. ; Должен 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 в соответствии с требованиями нормативно правовых актов и нормативных методических документов. ; Должен владеть навыками конфигурирования локальных сетей, навыками реализации сетевых протоколов с помощью программных средств; навыками настройки межсетевых экранов; навыками применения нормативно правовых актов и нормативных методических документов в области инфокоммуникационных систем; методикой анализа сетевого трафика; методикой анализа результатов работы средств обнаружения вторжений. ;
ПК-17	способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации	
ПК-14	способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации	
ПК-3	способностью проводить анализ защищенности автоматизированных систем	

Общие характеристики показателей и критериев оценивания компетенций на всех этапах

Согласована на портале № 15401

приведены в таблице 2.

Таблица 2 – Общие характеристики показателей и критериев оценивания компетенций по этапам

Показатели и критерии	Знать	Уметь	Владеть
Отлично (высокий уровень)	Обладает фактическими и теоретическими знаниями в пределах изучаемой области с пониманием границ применимости	Обладает диапазоном практических умений, требуемых для развития творческих решений, абстрагирования проблем	Контролирует работу, проводит оценку, совершенствует действия работы
Хорошо (базовый уровень)	Знает факты, принципы, процессы, общие понятия в пределах изучаемой области	Обладает диапазоном практических умений, требуемых для решения определенных проблем в области исследования	Берет ответственность за завершение задач в исследовании, приспосабливает свое поведение к обстоятельствам в решении проблем
Удовлетворительно (пороговый уровень)	Обладает базовыми общими знаниями	Обладает основными умениями, требуемыми для выполнения простых задач	Работает при прямом наблюдении

2 Реализация компетенций

2.1 Компетенция ПК-26

ПК-26: способностью администрировать подсистему информационной безопасности автоматизированной системы.

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования компетенции, применяемые для этого виды занятий и используемые средства оценивания представлены в таблице 3.

Таблица 3 – Этапы формирования компетенции и используемые средства оценивания

Состав	Знать	Уметь	Владеть
Содержание этапов	устройство подсистемы информационной безопасности автоматизированных систем	администрировать подсистему информационной безопасности автоматизированной системы	способностью администрировать подсистему информационной безопасности автоматизированной системы
Виды занятий	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Интерактивные лекции; • Практические занятия; • Лабораторные работы; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Интерактивные лекции; • Практические занятия; • Лабораторные работы; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Лабораторные работы; • Самостоятельная работа;

Согласована на портале № 15401

Используемые средства оценивания	• Отчет по лабораторной работе; • Опрос на занятиях; • Зачет; • Экзамен;	• Отчет по лабораторной работе; • Опрос на занятиях; • Зачет; • Экзамен;	• Отчет по лабораторной работе; • Зачет; • Экзамен;

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 4.

Таблица 4 – Показатели и критерии оценивания компетенции на этапах

Состав	Знать	Уметь	Владеть
Отлично (высокий уровень)	• Устройство подсистем информационной безопасности и принципы их проектирования;	• администрировать подсистему информационной безопасности автоматизированной системы и осуществлять контроль;	• способностью администрировать подсистему информационной безопасности автоматизированной системы и осуществлять контроль;
Хорошо (базовый уровень)	• Устройство подсистем информационной безопасности;	• администрировать подсистему информационной безопасности автоматизированной системы ;	• способностью администрировать подсистему информационной безопасности автоматизированной системы;
Удовлетворительно (пороговый уровень)	• Основы устройства подсистем информационной безопасности;	• администрировать подсистему информационной безопасности автоматизированной системы под прямым наблюдением;	• способностью администрировать подсистему информационной безопасности автоматизированной системы под прямым наблюдением;

2.2 Компетенция ПК-17

ПК-17: способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации.

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования компетенции, применяемые для этого виды занятий и используемые средства оценивания представлены в таблице 5.

Таблица 5 – Этапы формирования компетенции и используемые средства оценивания

Состав	Знать	Уметь	Владеть
Содержание этапов	Методы проведения инструментального мониторинга защищенности информации в автоматизированной системе и выявления каналов утечки информации	проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации	способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации
Виды занятий	• Интерактивные	• Интерактивные	• Интерактивные

Согласована на портале № 15401

	лабораторные занятия; • Интерактивные лекции; • Лабораторные работы; • Лекции; • Самостоятельная работа; • Интерактивные практические занятия; • Практические занятия;	лабораторные занятия; • Интерактивные лекции; • Лабораторные работы; • Лекции; • Самостоятельная работа; • Интерактивные практические занятия; • Практические занятия;	лабораторные занятия; • Лабораторные работы; • Самостоятельная работа; • Интерактивные практические занятия;
Используемые средства оценивания	• Отчет по лабораторной работе; • Опрос на занятиях; • Зачет; • Экзамен;	• Отчет по лабораторной работе; • Опрос на занятиях; • Зачет; • Экзамен;	• Отчет по лабораторной работе; • Зачет; • Экзамен;

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 6.

Таблица 6 – Показатели и критерии оценивания компетенции на этапах

Состав	Знать	Уметь	Владеть
Отлично (высокий уровень)	• Методы проведения инструментального мониторинга защищенности информации в автоматизированной системе и выявления каналов утечки информации;	• Проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации;	• Способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации;
Хорошо (базовый уровень)	• Методы выявления каналов утечки информации и основные методы проведения инструментального мониторинга защищенности информации в автоматизированной системе;	• Проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации под наблюдением более опытного специалиста;	• Способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации под наблюдением более опытного специалиста;
Удовлетворительно (пороговый уровень)	• Основные методы выявления каналов утечки информации;	• Выявлять каналы утечки информации;	• Способностью выявлять каналы утечки информации;

2.3 Компетенция ПК-14

ПК-14: способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации.

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования

Согласована на портале № 15401

компетенции, применяемые для этого виды занятий и используемые средства оценивания представлены в таблице 7.

Таблица 7 – Этапы формирования компетенции и используемые средства оценивания

Состав	Знать	Уметь	Владеть
Содержание этапов	Методы проведения контрольных проверок работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации	Проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации	Способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации
Виды занятий	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Интерактивные лекции; • Практические занятия; • Лабораторные работы; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Интерактивные лекции; • Практические занятия; • Лабораторные работы; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Интерактивные лабораторные занятия; • Лабораторные работы; • Самостоятельная работа;
Используемые средства оценивания	• Отчет по лабораторной работе; • Опрос на занятиях; • Зачет; • Экзамен;	• Отчет по лабораторной работе; • Опрос на занятиях; • Зачет; • Экзамен;	• Отчет по лабораторной работе; • Зачет; • Экзамен;

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 8.

Таблица 8 – Показатели и критерии оценивания компетенции на этапах

Состав	Знать	Уметь	Владеть
Отлично (высокий уровень)	• Методы проведения контрольных проверок работоспособности применяемых средств защиты информации, а также принципы их применения.;	• Проводить контрольные проверки работоспособности применяемых средств защиты информации и осуществлять контроль;	• Способностью проводить контрольные проверки работоспособности применяемых средств защиты информации и осуществлять контроль выполнения таких проверок;
Хорошо (базовый уровень)	• Методы проведения контрольных проверок работоспособности применяемых средств защиты информации;	• Проводить контрольные проверки работоспособности применяемых средств защиты информации;	• Способностью проводить контрольные проверки работоспособности применяемых средств защиты информации;

Согласована на портале № 15401

Удовлетворительно (пороговый уровень)	• Базовые методы проведения контрольных проверок работоспособности применяемых средств защиты информации;	• Проводить контрольные проверки работоспособности применяемых средств защиты информации под прямым наблюдением более опытного специалиста;	• Способностью проводить контрольные проверки работоспособности применяемых средств защиты информации под прямым наблюдением более опытного специалиста;

2.4 Компетенция ПК-3

ПК-3: способностью проводить анализ защищенности автоматизированных систем.

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования компетенции, применяемые для этого виды занятий и используемые средства оценивания представлены в таблице 9.

Таблица 9 – Этапы формирования компетенции и используемые средства оценивания

Состав	Знать	Уметь	Владеть
Содержание этапов	Методы анализа защищенности автоматизированных систем	Проводить анализ защищенности автоматизированных систем	Способностью проводить анализ защищенности автоматизированных систем
Виды занятий	• Интерактивные лабораторные занятия; • Интерактивные лекции; • Лабораторные работы; • Лекции; • Самостоятельная работа; • Интерактивные практические занятия; • Практические занятия;	• Интерактивные лабораторные занятия; • Интерактивные лекции; • Лабораторные работы; • Лекции; • Самостоятельная работа; • Интерактивные практические занятия; • Практические занятия;	• Интерактивные лабораторные занятия; • Лабораторные работы; • Самостоятельная работа; • Интерактивные практические занятия;
Используемые средства оценивания	• Отчет по лабораторной работе; • Опрос на занятиях; • Зачет; • Экзамен;	• Отчет по лабораторной работе; • Опрос на занятиях; • Зачет; • Экзамен;	• Отчет по лабораторной работе; • Зачет; • Экзамен;

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 10.

Таблица 10 – Показатели и критерии оценивания компетенции на этапах

Состав	Знать	Уметь	Владеть
Отлично (высокий уровень)	• Методы анализа защищенности автоматизированных систем, а также принципы создания таких методов;	• Проводить анализ защищенности автоматизированных систем и осуществлять контроль проведения;	• Способностью проводить анализ защищенности автоматизированных систем и осуществлять контроль работ;
Хорошо (базовый	• Методы анализа	• Проводить анализ	• Способностью

Согласована на портале № 15401

уровень)	защищенности автоматизированных систем;	защищенности автоматизированных систем;	проводить анализ защищенности автоматизированных систем;
Удовлетворительно (пороговый уровень)	• Базовые методы анализа защищенности автоматизированных систем;	• Проводить анализ защищенности автоматизированных систем под прямым наблюдением более опытного специалиста;	• Способностью проводить анализ защищенности автоматизированных систем под прямым наблюдением более опытного специалиста;

3 Типовые контрольные задания

Для реализации вышеперечисленных задач обучения используются типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы, в следующем составе.

3.1 Темы опросов на занятиях

– История развития сетей ЭВМ. Место и роль вычислительных сетей в современном мире. Основные понятия и терминология. Общие представления о вычислительной сети. Общее понятие об иерархической структуре протоколов. Принципы многоуровневой организации локальных и глобальных сетей ЭВМ. Модель OSI. Стандартные стеки коммуникационных протоколов.

– Стандартизация в сетях. Классификация вычислительных сетей. Требования, предъявляемые к современным вычислительным сетям. Методы и технологии проектирования средств телекоммуникаций. Структуризации сети. Физическая и логическая топологии сетей. Основное коммуникационное оборудование

– Каналы связи. Характеристики каналов связи. Логическое кодирование. Асинхронная и синхронная передачи. Иерархия в кабельной системе. Структурированная кабельная система.

– Конфигурации локальных вычислительных сетей и методы доступа в них. Структура и функции локальных сетей. Содержание стандарта IEEE 802. Базовые технологии локальных сетей. IEEE 802.2 Ethernet. Оборудование локальных сетей.

– Программные средства телекоммуникации. Структура программного обеспечения локальной сети. Классификация программного обеспечения локальных сетей. Принципы построения сетевого программного обеспечения и сетевых операционных систем. Классификация серверов. Проектирование сетей ЭВМ по принципу «клиент-сервер».

– Сетевой уровень передачи данных. IP-адресация. Реализация межсетевого взаимодействия средствами TCP/IP. Порядок распределения IP-адресов. Отображение IP-адресов на локальные адреса. ARP протокол.

– Принципы маршрутизации в IP-сетях. Протоколы маршрутизации. Понятие домена. Доменная адресация в IP-сетях. DNS протокол.

– Протокол IPv6. Протоколы транспортного уровня TCP и UDP.

– Современные тенденции развития телекоммуникационных систем. Интеграция различных типов сетей и сетевых служб. Виртуализация информационных систем. Облачные вычисления.

– Обеспечение безопасности телекоммуникационных связей и административный контроль. Основные понятия и терминология.

– Типовые угрозы сетевой безопасности. Основы классификации сетевых угроз и атак. Влияние человеческого фактора на сетевую безопасность.

– Защита топологии сети. Виртуальные локальные сети. Дополнительные функции коммутаторов. Персональные экраны. Абонентское шифрование.

– Защита сетевого трафика и компонентов сети. Защита компонентов сети от НСД. Безопасность ресурсов сети. Средства идентификации и аутентификации, методы разделения ресурсов и технологии разграничения доступа.

Согласована на портале № 15401

– Средства повышения надежности функционирования сетей. Защита от сбоев электропитания, аппаратного и программного обеспечения. Контроль и распределение нагрузки на вычислительную сеть.

– Регламентирующие документы в области безопасности вычислительных сетей. Стандарты безопасности вычислительных сетей и их компонентов. Правовые основы защиты информации в сетях.

– Сетевые операционные системы Windows, Unix/Linux. Основные протоколы, службы, функционирование, средства обеспечения безопасности, средства управления и контроля.

– Политика безопасности: Понятие политики безопасности. Типовые элементы политики безопасности. Построение, реализация, поддержание и модификация политики безопасности.Критерии оценки безопасности сетевых ОС. Основные критерии анализа сетевой безопасности. Общая процедура анализа.

– Основные механизмы обеспечения безопасности и управления распределенными ресурсами. Обеспечение надежности инфраструктуры Интернет.

– Защита каналов связи в Интернет. Виды используемых в Интернет каналов связи. Использование межсетевых экранов. Виртуальные частные сети.

– Уязвимости и защита базовых протоколов и служб: Протоколы маршрутизации. Семейство TCP/IP. Службы поиска. Безопасность WWW и электронной почты.

– Системы обнаружения и противодействия вторжениям. Классификация и принципы функционирования систем обнаружения вторжений. Сканеры безопасности.

– Классы сканеров безопасности и особенности применения. Защита от вирусов. Защита электронного документооборота.

3.2 Экзаменационные вопросы

– 1. Типовые конфигурации информационных систем. Влияние конфигурации информационной системы на безопасность хранимых, обрабатываемых и передаваемых по сети данных. 2. Угроза. Уязвимость. Атака. Взаимосвязь между этими понятиями. 3. Классификация угроз информационной безопасности вычислительных сетей. 4. Классификация уязвимостей. 5. Классификация атак. 6. Перехват информации в сети. Инструменты. Способы противодействия перехвату. 7. Spoofing. Способы подделки идентификаторов. Способы противодействия spoofing`y. 8. DOS-атаки. Особенности реализации. Способы противодействия DOS-атакам. 9. Универсальные методы обеспечения информационной безопасности компьютеров и компьютерных сетей. 10. Специализированные методы обеспечения информационной безопасности компьютерных сетей. 11. Идентификация и аутентификация. Особенности аутентификации пользователей в компьютерных сетях. 12. Протокол Kerberos. Назначение. Особенности функционирования. 13. Разграничение доступа к информационным ресурсам компьютерных сетей. 14. Криптографическая защита информации в компьютерных сетях. Достоинства и недостатки. Способы преодоления криптографической защиты информации. 15. Электронная подпись. Назначение. Применение для защиты сетевого взаимодействия. Примеры. 16. Сканеры безопасности. Способы выявления уязвимостей в информационных системах. 17. Аудит в информационных системах. Функции и назначение аудита, его роль в обеспечении информационной безопасности. 18. Системы обнаружения вторжений. Системы предотвращения вторжений. Методики выявления сетевых атак. 19. Сетевые и хостовые системы обнаружения и предотвращения вторжений. Достоинства и недостатки. 20. Межсетевые экраны. Классификация. Варианты размещения межсетевого экрана. Достоинства и недостатки. 21. Демилитаризованная зоны. Назначение. Способы выделения. 22. Классификация межсетевых экранов по уровням защищенности. Показатель защищенности, применяемые для классификации. Применение межсетевых экранов различных классов. 23. Технология VPN (Виртуальные частные сети). Назначение. Достоинства и недостатки. 24. Основные компоненты технологии виртуальных частных сетей (VLAN). 25. Вредоносные программы. Классификация. Каналы распространения. Влияние на информационные системы. 26. Антивирусные средства. Классификация. Методики выявления вредоносного кода. 27. Средства обеспечения информационной безопасности в ОС Windows’2003. Разграничение доступа к данным. Групповая политика. Область действия групповых политик. 28. Основные этапы разработки защищенной компьютерной сети. 29. Проблемы обеспечения безопасности

Согласована на портале № 15401

прикладных сервисов (Веб, почта, FTP) и их решения. 30. Физические средства обеспечения информационной безопасности.

3.3 Темы лабораторных работ

– Моделирование сетевых устройств и протоколов в локальных сетях

– Моделирование виртуальных локальных сетей (VLAN) с разграничением доступа к сетевым ресурсам

– Настройка подключения узла к сети. Автоматическая динамическая и статическая настройки сетевого подключения.

– Стек протоколов TCP/IP. Прикладные протоколы сети Интернет.

– Сети Microsoft Windows. Управление сетевыми ресурсами в одноранговой сети.

– Сети Microsoft Windows. Active Directory. Управление сетевыми ресурсами корпоративной сети. Групповые политики.

– Моделирование базовых служб и протоколов маршрутизации в глобальных сетях.

– Базовые службы сети Интернет. DHCP. DNS. Протоколы маршрутизации.

– Прикладные службы сети Интернет. Настройка Web-, FTP-серверов и сервера электронной почты.

– Разграничение доступа к локальным и сетевым ресурсам. Дискреционная и мандатная модели управления доступом.

– Инструменты для исследования сети (сниферы)

– Инструменты для исследования сети (сканеры безопасности)

– Межсетевые экраны

– Антивирусная защита

– Виртуальные частные сети

– Системы обнаружения и предотвращения вторжений

– DLP-системы

– Безопасность прикладных протоколов

3.4 Зачёт

– 1. Понятие сети. Требования, предъявляемые к сети. 2. Классификация сетей. Признаки классификации. 3. Сетевые топологии. Преимущества и недостатки базовых сетевых топологий. 4. Методы коммутации узлов сети. Преимущества и недостатки различных методов коммутации. 5. Методы адресации в малых и больших сетях. Требования к адресам. 6. Основные аппаратные и программные компоненты компьютерных сетей 7. Назначение и состав линий связи. Назначение каждого компонента линий связи. 8. Основные виды передающих сред. Их характеристики. Ограничения передающих сред. 9. Беспроводная линия связи. Состав оборудования. Понятие канала. 10. Сетевая модель OSI. Назначение. Уровни взаимодействия открытых систем. 11. Стандартизация сетей. Проект 802.x. 12. Методы доступа к среде передачи данных. 13. Понятие протокола и интерфейса. Стеки протоколов. Стандартные стеки протоколов. 14. Сетевая архитектура Ethernet. Базовый стандарт. Компоненты реализации на физическом уровне. 15. Структура кадра технологии Ethernet. Технология VLAN. Стандарт IEEE 802.1q. 16. Сетевая архитектура Token Ring. 17. Сетевая архитектура FDDI. 18. Оборудование ЛВС. Принципы работы концентраторов, мостов, коммутаторов. 19. Сетевые операционные системы. Требования, предъявляемые к сетевым ОС. 20. Базовые примитивы передачи сообщений в распределенной сети. Вызов удаленных процедур. Механизм сокетов. 21. Сетевые файловые системы. Семантика разделения файлов. 22. Службы именования ресурсов. Служба каталогов. Доменный подход. 23. Служба каталогов Active Directory. Управление объектами сети. Групповые политики. 24. Задачи построения объединенных сетей. 25. Глобальная сеть Интернет. Построение. Основные понятия. Семейство протоколов TCP/IP и его роль в построении глобальных сетей. 26. Стек протоколов TCP/IP. Область применения. Основные характеристики. 27. Типы адресов, применяемых в сети Интернет. Назначение. Технологии разрешения адресов. 28. IP-адреса. Классы IP-сетей. 29. IP-адреса. Технология CIDR. Понятие сетевого префикса. 30. Оборудование ГВС. Краткая характеристика и назначение. 31. Структура сети Интернет. Автономные системы и Магистральные сети. Типы протоколов маршрутизации. 32. Маршрутизация IP-протокола.

Согласована на портале № 15401

Алгоритмы маршрутизации. 33. Протоколы маршрутизации RIP и OSPF. Характеристики, достоинства и недостатки. 34. Протокол ARP. Назначение. Принцип функционирования. 35. Протокол DHCP. Назначение. Принцип функционирования. 36. Служба DNS. Назначение. Принцип функционирования. 37. Протоколы транспортного уровня стека TCP/IP. Сравнительные характеристики и принципы работы. 38. Перехват пакетов в локальной сети. Инструменты. Структура пакетов. 39. Технологии «последней мили». Программный и аппаратный состав. 40. Службы WWW и FTP. Протоколы. Настройки серверного и клиентского ПО. 41. Служба E-mail. Протоколы электронной почты. Настройки серверного и клиентского ПО. 42. Служба мгновенных сообщений Jabber. Протоколы. Настройки серверного и клиентского ПО. 43. Технологии передачи голосовой информации. Протоколы SIP, RTP. 44. Типовая структура отказоустойчивого кластера. Резервирование данных. 45. Основные команды, используемые при работе с сетью в режиме командной строки.

4 Методические материалы

Для обеспечения процесса обучения и решения задач обучения используются следующие материалы:

– методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы фор-мирования компетенций, согласно п. 12 рабочей программы.

4.1. Основная литература

1. Компьютерные сети: Принципы, технологии, протоколы [Текст] : учебник для вузов / В. Г. Олифер, Н. А. Олифер. - 4-е изд. - СПб. : ПИТЕР, 2013. - 944 с. : ил., табл. - (Учебник для вузов. Стандарт третьего поколения). - Алф. указ.: с. 918-943. - ISBN 978-5-496-00004-8 : 470.69 р. (наличие в библиотеке ТУСУР - 20 экз.)

2. Компьютерные сети [Текст] : научное издание / Э. Таненбаум, Д. Уэзеролл. - 5-е изд. - СПб. : ПИТЕР, 2013. - 960 с. : ил., табл. - (КЛАССИКА COMPUTER SCIENCE). - Пер. с англ. - Алф. указ.: с. 947-955. - ISBN 978-5-4461-0068-2 : 1244.32 р. (наличие в библиотеке ТУСУР - 15 экз.)

4.2. Дополнительная литература

1. Сетевые операционные системы : Учебное пособие для вузов / В. Г. Олифер, Н. А. Олифер. - СПб. : Питер, 2007. - 538[6] с. : ил. - (Учебник для вузов). - Библиогр.: с. 525-526. - Алф. указ.: с. 527-538. - ISBN 5-272-00120-6 : 145.20 р. (наличие в библиотеке ТУСУР - 10 экз.)

4.3. Обязательные учебно-методические пособия

1. Безопасность сетей ЭВМ: Методические указания для лабораторных и практических работ / Новохрестов А. К., Праскурин Г.А., 2014. – 99 с. [Электронный ресурс] [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/work_progs/nak/BSEVM_lab_pract.pdf

2. Безопасность сетей ЭВМ: Методические указания для самостоятельной работы студента / Новохрестов А.К., Праскурин Г.А., 2014. – 4 с. [Электронный ресурс] [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/work_progs/nak/BSEVM_sam.pdf

4.4. Базы данных, информационно справочные и поисковые системы

1. http://www.lib.tusur.ru – библиотека университета;
2. http://www.elibrary.ru – научная электронная библиотека;
3. http://www.edu.ru – веб-сайт системы федеральных образовательных порталов.
4.
5. Программное обеспечение:
6. операционные системы семейства Windows;
7. средство защиты информации "Блокхост-сеть К";
8. система обнаружения вторжений "Snort";
9. средство моделирования сетей Cisco Packet Tracer;
10. DLP-система "Контур информационной безопасности SearchInform";
11. дистрибутив Kali Linux;
12. система анализа защищенности сети "MaxPatrol".

Согласована на портале № 15401