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

Информационная безопасность в локальных и распределенных вычислительных сетях

Уровень образования: **высшее образование - специалитет**
Направление подготовки (специальность): **38.05.01 Экономическая безопасность**
Направленность (профиль): **Экономико-правовое обеспечение экономической 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 2017

Согласована на портале № 19336

Рассмотрена и одобрена на заседании кафедры
протокол № 4 от « 3 » 5 2017 г.

ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 38.05.01 Экономическая безопасность, утвержденного 16 января 2017 года, рассмотрена и утверждена на заседании кафедры «___» _____ 20__ года, протокол №_____.

Разработчик:

ассистент каф. КИБЭВС _____ А. К. Новохрестов

Заведующий обеспечивающей каф.
КИБЭВС _____ А. А. Шелупанов

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

Декан ФБ _____ Е. М. Давыдова

Заведующий выпускающей каф.
КИБЭВС _____ А. А. Шелупанов

Эксперт:

доцент каф. КИБЭВС _____ А. А. Конев

Согласована на портале № 19336

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 «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 следующие дисциплины: Информатика, Основы информационной безопасности.

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 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 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

Согласована на портале № 19336

Самостоятельная работа (всего)	108	108
Проработка лекционного материала	13	13
Подготовка к практическим занятиям, семинарам	95	95
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	Лекции	Практические занятия	Самостоятельная работа	Всего часов (без экзамена)	Формируемые компетенции
8 семестр					
1 Основные понятия информационных сетей	4	0	7	11	ПСК-2
2 Основы построения современных локальных сетей	4	16	20	40	ПСК-2
3 Средства реализации межсетевого взаимодействия	6	12	18	36	ПСК-2
4 Перспективные направления развития и проблемы информационных сетей	2	0	1	3	ПСК-2
5 Основные понятия информационной безопасности	4	0	1	5	ПСК-2
6 Технологии обеспечения безопасности в локальных сетях	4	12	20	36	ПСК-2
7 Обеспечение безопасности сетей на базе сетевых операционных систем	2	0	1	3	ПСК-2
8 Обеспечение безопасности межсетевого взаимодействия	6	32	39	77	ПСК-2
9 Правовые основы защиты информации в компьютерных сетях. Защищенный документооборот	4	0	1	5	ПСК-2
Итого за семестр	36	72	108	216	
Итого	36	72	108	216	

Согласована на портале № 19336

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 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	ПСК-2
	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. Иерархия в кабельной системе. Структурированная кабельная система.	2	ПСК-2
	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 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	ПСК-2
	Принципы маршрутизации в IP-сетях. Протоколы маршрутизации. Понятие	2	

Согласована на портале № 19336

	домена. Доменная адресация в IP-сетях. DNS протокол.		
	Протокол IPv6. Протоколы транспортного уровня TCP и UDP.	2	
	Итого	6	
4 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	ПСК-2
	Итого	2	
5 Основные понятия информационной безопасности	Обеспечение безопасности телекоммуникационных связей и административный контроль. Основные понятия и терминология.	2	ПСК-2
	Типовые угрозы сетевой безопасности. Основы классификации сетевых угроз и атак. Влияние человеческого фактора на сетевую безопасность.	2	
	Итого	4	
6 Технологии обеспечения безопасности в локальных сетях	Защита топологии сети. Виртуальные локальные сети. Дополнительные функции коммутаторов. Персональные экраны. Абонентское шифрование.	2	ПСК-2
	Регламентирующие документы в области безопасности вычислительных сетей. Стандарты безопасности вычислительных сетей и их компонентов. Правовые основы защиты информации в сетях.	2	
	Итого	4	
7 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	ПСК-2
	Итого	2	
8 Обеспечение безопасности межсетевого взаимодействия	Основные механизмы обеспечения безопасности и управления распределенными ресурсами. Обеспечение надежности инфраструктуры Интернет.	2	ПСК-2
	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 поис-	2	

Согласована на портале № 19336

	ка. Безопасность WWW и электронной почты.		
	Итого	6	
9 Правовые основы защиты информации в компьютерных сетях. Защищенный документооборот	Системы обнаружения и противодействия вторжениям. Классификация и принципы функционирования систем обнаружения вторжений. Сканеры безопасности.	2	ПСК-2
	Классы сканеров безопасности и особенности применения. Защита от вирусов.Защита электронного документооборота.	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	8	9
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

Компетенции	Виды занятий			Формы контроля
	Лекции	Практические занятия	Самостоятельная работа	
ПСК-2	+	+	+	Отчет по лабораторной работе, Опрос на занятиях, Отчет по практическому занятию

6. Интерактивные методы и формы организации обучения

Не предусмотрено РУП

Согласована на портале № 19336

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			
2 Основы построения современных локальных сетей	Настройка подключения узла к сети. Автоматическая динамическая и статическая настройки сетевого подключения.	4	ПСК-2
	Стек протоколов TCP/IP. Прикладные протоколы сети Интернет.	4	
	Сети Microsoft Windows. Управление сетевыми ресурсами в одноранговой сети.	4	
	Сети Microsoft Windows. Управление сетевыми ресурсами в одноранговой сети.	4	
	Итого	16	
3 Средства реализации межсетевого взаимодействия	Моделирование базовых служб и протоколов маршрутизации в глобальных сетях.	4	ПСК-2
	Базовые службы сети Интернет. DHCP. DNS. Протоколы маршрутизации.	4	
	Прикладные службы сети Интернет. Настройка Web-, FTP-серверов и сервера электронной почты.	4	
	Итого	12	
6 Технологии обеспечения безопасности в локальных сетях	Разграничение доступа к локальным и сетевым ресурсам. Дискреционная и мандатная модели управления доступом.	4	ПСК-2
	Инструменты для исследования сети (сниферы)	4	
	Инструменты для исследования сети (сканеры безопасности)	4	
	Итого	12	
8 Обеспечение безопасности межсетевого взаимодействия	Межсетевые экраны	4	ПСК-2
	Антивирусная защита	4	
	Виртуальные частные сети	8	
	Системы обнаружения и предотвраще-	4	

Согласована на портале № 19336

	ния вторжений		
	DLP-системы	8	
	Безопасность прикладных протоколов	4	
	Итого	32	
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 информационных сетей	Подготовка к практическим занятиям, семинарам	5	ПСК-2	Опрос на занятиях, Отчет по практическому занятию
	Проработка лекционного материала	2		
	Итого	7		
2 Основы построения современных локальных сетей	Подготовка к практическим занятиям, семинарам	18	ПСК-2	Опрос на занятиях, Отчет по практическому занятию
	Проработка лекционного материала	2		
	Итого	20		
3 Средства реализации межсетевого взаимодействия	Подготовка к практическим занятиям, семинарам	15	ПСК-2	Опрос на занятиях, Отчет по практическому занятию
	Проработка лекционного материала	3		
	Итого	18		
4 Перспективные направления развития и проблемы информационных сетей	Проработка лекционного материала	1		Опрос на занятиях
	Итого	1		
5 Основные понятия информационной безопасности	Проработка лекционного материала	1		Опрос на занятиях
	Итого	1		
6 Технологии обеспечения безопасности в локальных сетях	Подготовка к практическим занятиям, семинарам	19	ПСК-2	Опрос на занятиях, Отчет по практическому занятию
	Проработка лекционного материала	1		

Согласована на портале № 19336

	Итого	20		
7 Обеспечение безопасности сетей на базе сетевых операционных систем	Проработка лекционного материала	1		Опрос на занятиях
	Итого	1		
8 Обеспечение безопасности межсетевого взаимодействия	Подготовка к практическим занятиям, семинарам	38	ПСК-2	Опрос на занятиях, Отчет по практическому занятию
	Проработка лекционного материала	1		
	Итого	39		
9 Правовые основы защиты информации в компьютерных сетях. Защищенный документооборот	Проработка лекционного материала	1		Опрос на занятиях
	Итого	1		
Итого за семестр		108		
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
8 семестр				
Опрос на занятиях	3	4	3	10
Отчет по практическому занятию	30	30	30	90
Итого максимум за период	33	34	33	100
Нарастающим итогом	33	67	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.

Согласована на портале № 19336

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

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.

Согласована на портале № 19336

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 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

Согласована на портале № 19336

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-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 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:

Согласована на портале № 19336

– 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 № 19336

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

Информационная безопасность в локальных и распределенных вычислительных сетях

Уровень образования: **высшее образование - специалитет**
Направление подготовки (специальность): **38.05.01 Экономическая безопасность**
Направленность (профиль): **Экономико-правовое обеспечение экономической 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

Разработчик:
- ассистент каф. КИБЭВС А. К. Новохрестов

Дифференцированный зачет: 8 семестр

Томск 2017

Согласована на портале № 19336

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

Общие характеристики показателей и критериев оценивания компетенций на всех этапах приведены в таблице 2.

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

Показатели и критерии	Знать	Уметь	Владеть

Согласована на портале № 19336

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 ПСК-2

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

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	условия, способствующие совершению правонарушений в отношении сведений, составляющих государственную, банковскую, коммерческую тайну, персональных данных, других сведений ограниченного доступа	выявлять условия, способствующие совершению правонарушений в отношении сведений, составляющих государственную, банковскую, коммерческую тайну, персональных данных, других сведений ограниченного доступа	навыками выявления условий, способствующих совершению правонарушений в отношении сведений, составляющих государственную, банковскую, коммерческую тайну, персональных данных, других сведений ограниченного доступа
Виды занятий	• Практические занятия; • Лекции; • Самостоятельная работа;	• Практические занятия; • Лекции; • Самостоятельная работа;	• Самостоятельная работа;
Используемые средства оценивания	• Отчет по лабораторной работе; • Опрос на занятиях; • Отчет по практическому занятию; • Дифференцированный зачет;	• Отчет по лабораторной работе; • Опрос на занятиях; • Отчет по практическому занятию; • Дифференцированный зачет;	• Отчет по лабораторной работе; • Отчет по практическому занятию; • Дифференцированный зачет;

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

Согласована на портале № 19336

Таблица 4 – Показатели и критерии оценивания компетенции на этапах

Состав	Знать	Уметь	Владеть
Отлично (высокий уровень)	• знает в полном объеме условия, способствующие совершению правонарушений в отношении сведений ограниченного доступа;	• умеет в полном объеме выявлять условия, способствующие совершению правонарушений в отношении сведений ограниченного доступа;	• в полном объеме владеет навыками выявления условий, способствующих совершению правонарушений в отношении сведений ограниченного доступа;
Хорошо (базовый уровень)	• знает на продвинутом уровне условия, способствующие совершению правонарушений в отношении сведений ограниченного доступа;	• умеет на продвинутом уровне выявлять условия, способствующие совершению правонарушений в отношении сведений ограниченного доступа;	• на продвинутом уровне владеет навыками выявления условий, способствующих совершению правонарушений в отношении сведений ограниченного доступа;
Удовлетворительно (пороговый уровень)	• знает на базовом уровне условия, способствующие совершению правонарушений в отношении сведений ограниченного доступа;	• умеет на базовом уровне выявлять условия, способствующие совершению правонарушений в отношении сведений ограниченного доступа;	• на базовом уровне владеет навыками выявления условий, способствующих совершению правонарушений в отношении сведений ограниченного доступа;

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.

– 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 вычисле-

Согласована на портале № 19336

ния.

– 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.

– 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.

– 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 Вопросы для подготовки к практическим занятиям, семинарам

– 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. Управление сетевыми ресурсами в одноранговой сети.

– 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.

– Инструменты для исследования сети (сниферы)

– Инструменты для исследования сети (сканеры безопасности)

– Антивирусная защита

– Виртуальные частные сети

– Системы обнаружения и предотвращения вторжений

– DLP-системы

– Безопасность прикладных протоколов

3.3 Темы лабораторных работ

– 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. Управление сетевыми ресурсами в одноранговой сети.

– 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.

– Инструменты для исследования сети (сниферы)

– Инструменты для исследования сети (сканеры безопасности)

Согласована на портале № 19336

- Антивирусная защита
- Виртуальные частные сети
- Системы обнаружения и предотвращения вторжений
- DLP-системы
- Безопасность прикладных протоколов

3.4 Вопросы дифференцированного зачета

- 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. 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.)

Согласована на портале № 19336

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 № 19336