МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

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

УТВЕРЖДАЮ
Директор департамента образования
_____ П. Е. Троян
«___» _____ 20__ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Безопасность сетей ЭВМ

Уровень образования: **высшее образование - бакалавриат**
Направление подготовки / специальность: **10.03.01 Информационная безопасность**
Направленность (профиль) / специализация: **Безопасность автоматизированных 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	0	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	18	36	часов
7	Всего (без экзамена)	72	108	180	часов
8	Подготовка и сдача экзамена	0	36	36	часов
9	Общая трудоемкость	72	144	216	часов
		2.0	4.0	6.0	З.Е.

Зачет: 5 семестр
Экзамен: 6 семестр

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Шелупанов А.А.
Должность: Ректор
Дата подписания: 23.08.2017
Уникальный программный ключ:
c53e145e-8b20-45aa-9347-a5e4dbb90e8d

Томск 2018

Согласована на портале № 47275

Рассмотрена и одобрена на заседании кафедры
протокол № от «___» _____ 20__ г.

ЛИСТ СОГЛАСОВАНИЯ

Рабочая программа дисциплины составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 10.03.01 Информационная безопасность, утвержденного 01.12.2016 года, рассмотрена и одобрена на заседании кафедры КИБЭВС «___» _____ 20__ года, протокол №_____.

Разработчики:

преподаватель каф. КИБЭВС	_____	А. К. Новохрестов
доцент каф. КИБЭВС	_____	А. А. Конев

Заведующий обеспечивающей каф. КИБЭВС	_____	А. А. Шелупанов

Рабочая программа дисциплины согласована с факультетом и выпускающей кафедрой:

Декан ФБ	_____	Е. М. Давыдова
Заведующий выпускающей каф. КИБЭВС	_____	А. А. Шелупанов

Эксперты:

доцент каф. КИБЭВС	_____	Е. Ю. Костюченко
доцент каф. КИБЭВС	_____	К. С. Сарин

Согласована на портале № 47275

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.32) относится к блоку 1 (базовая часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Безопасность сетей ЭВМ, Информатика, Основы информационной безопасности.

Последующими дисциплинами являются: Безопасность сетей ЭВМ.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ПК-2 способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач;

– ПК-6 способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации;

– ПК-15 способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;

– ОПК-7 способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты.

В результате изучения дисциплины обучающийся 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.

Согласована на портале № 47275

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	
		5 семестр	6 семестр
Аудиторные занятия (всего)	144	54	90
Лекции	46	18	28
Практические занятия	18	0	18
Лабораторные работы	80	36	44
Из них в интерактивной форме	40	16	24
Самостоятельная работа (всего)	36	18	18
Оформление отчетов по лабораторным работам	18	9	9
Проработка лекционного материала	14	9	5
Подготовка к практическим занятиям, семинарам	4	0	4
Всего (без экзамена)	180	72	108
Подготовка и сдача экзамена	36	0	36
Общая трудоемкость, ч	216	72	144
Зачетные Единицы	6.0	2.0	4.0

5. Содержание дисциплины

5.1. Разделы дисциплины и виды занятий

Разделы дисциплины и виды занятий приведены в таблице 5.1.

Таблица 5.1 – Разделы дисциплины и виды занятий

Названия разделов дисциплины	Лек., ч	Прак. зан., ч	Лаб. раб., ч	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
5 семестр						
1 Основные понятия информационных сетей	4	0	8	4	16	ПК-15, ПК-2
2 Основы построения современных локальных сетей	4	0	8	4	16	ПК-2, ОПК-7
3 Сетевые операционные системы	2	0	8	3	13	ПК-2
4 Средства реализации межсетевого взаимодействия	6	0	12	6	24	ПК-2
5 Перспективные направления развития и проблемы информационных сетей	2	0	0	1	3	ПК-2
Итого за семестр	18	0	36	18	72	
6 семестр						
6 Основные понятия	4	0	0	1	5	ПК-15, ПК-2,

Согласована на портале № 47275

информационной безопасности						ПК-6
7 Технологии обеспечения безопасности в локальных сетях	8	18	12	8	46	ПК-15, ПК-2, ПК-6, ОПК-7
8 Обеспечение безопасности сетей на базе сетевых операционных систем	6	0	0	1	7	ПК-15, ПК-2, ПК-6
9 Обеспечение безопасности межсетевого взаимодействия	6	0	32	7	45	ПК-15, ПК-2, ПК-6
10 Правовые основы защиты информации в компьютерных сетях. Защищенный документооборот	4	0	0	1	5	ПК-15, ПК-2, ПК-6
Итого за семестр	28	18	44	18	108	
Итого	46	18	80	36	180	

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-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	ПК-2, ОПК-7
	Конфигурации локальных вычислительных сетей и методы доступа в них. Структура и функции локальных сетей. Содержание стандарта IEEE 802. Базовые технологии локальных сетей.	2	

Согласована на портале № 47275

	IEEE 802.2 Ethernet. Оборудование локальных сетей.		
	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-2
	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-2
	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-2
	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-15, ПК-2, ПК-6
	Типовые угрозы сетевой безопасности. Основы классификации сетевых угроз и атак. Влияние человеческого фактора на сетевую безопасность.	2	
	Итого	4	
7 Технологии обеспечения безопасности в	Защита топологии сети. Виртуальные локальные сети. Дополнительные функции коммутаторов. Персональные	2	ПК-15, ПК-2, ПК-6, ОПК-7

Согласована на портале № 47275

локальных сетях	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.	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-2, ПК-6
	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 инфраструктуры Интернет.	2	ПК-15, ПК-2, ПК-6
	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	

Согласована на портале № 47275

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-15, ПК-2, ПК-6
	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 Безопасность сетей ЭВМ	+	+	+	+	+	+	+	+	+	+
2 Информатика	+									
3 Основы информационной безопасности						+				
Последующие дисциплины										
1 Безопасность сетей ЭВМ	+	+	+	+	+	+	+	+	+	+

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

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

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

Компетенции	Виды занятий				Формы контроля
	Лек.	Прак. зан.	Лаб. раб.	Сам. раб.	
ПК-2	+	+	+	+	Защита отчета, Отчет по лабораторной работе, Опрос на занятиях, Тест
ПК-6	+	+	+	+	Защита отчета, Отчет по лабораторной работе, Опрос на занятиях
ПК-15	+	+		+	Защита отчета, Опрос на занятиях

Согласована на портале № 47275

ОПК-7	+	+	+	+	Защита отчета, Отчет по лабораторной работе, Опрос на занятиях, Тест

6. Интерактивные методы и формы организации обучения

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

Таблица 6.1 – Технологии интерактивного обучения при разных формах занятий

Методы	Интерактивные лабораторные занятия, ч	Интерактивные лекции, ч	Интерактивные практические занятия, ч	Всего, ч
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.

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-2
	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-2, ОПК-7
	Стек протоколов TCP/IP. Прикладные протоколы сети Интернет.	4	
	Итого	8	

Согласована на портале № 47275

3 Сетевые операционные системы	Сети Microsoft Windows. Управление сетевыми ресурсами в одноранговой сети.	4	ПК-2
	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-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	
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-2, ПК-6, ОПК-7
	Инструменты для исследования сети (сниферы)	4	
	Инструменты для исследования сети (сканеры безопасности)	4	
	Итого	12	
9 Обеспечение безопасности межсетевого взаимодействия	Межсетевые экраны	4	ПК-2, ПК-6
	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	Построение структуры информационной сети, описание характера связей между	4	ПК-2, ОПК-7

Согласована на портале № 47275

безопасности в локальных сетях	элементами и информационных потоков.		
	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.

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-15, ПК-2	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-2, ОПК-7	Опрос на занятиях, Отчет по лабораторной работе
	Оформление отчетов по лабораторным работам	2		
	Итого	4		
3 Сетевые операционные системы	Проработка лекционного материала	1	ПК-2	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-2	Опрос на занятиях, Отчет по лабораторной работе
	Оформление отчетов по лабораторным работам	3		
	Итого	6		
5 Перспективные направления развития и проблемы	Проработка лекционного материала	1	ПК-2	Опрос на занятиях
	Итого	1		

Согласована на портале № 47275

информационных сетей				
Итого за семестр		18		
6 семестр				
6 Основные понятия информационной безопасности	Проработка лекционного материала	1	ПК-15, ПК-2, ПК-6	Опрос на занятиях
	Итого	1		
7 Технологии обеспечения безопасности в локальных сетях	Подготовка к практическим занятиям, семинарам	4	ПК-15, ПК-2, ПК-6, ОПК-7	Защита отчета, Опрос на занятиях, Отчет по лабораторной работе
	Проработка лекционного материала	1		
	Оформление отчетов по лабораторным работам	3		
	Итого	8		
8 Обеспечение безопасности сетей на базе сетевых операционных систем	Проработка лекционного материала	1	ПК-15, ПК-2, ПК-6	Опрос на занятиях
	Итого	1		
9 Обеспечение безопасности межсетевого взаимодействия	Проработка лекционного материала	1	ПК-15, ПК-2, ПК-6	Опрос на занятиях, Отчет по лабораторной работе
	Оформление отчетов по лабораторным работам	6		
	Итого	7		
10 Правовые основы защиты информации в компьютерных сетях. Защищенный документооборот	Проработка лекционного материала	1	ПК-15, ПК-2, ПК-6	Опрос на занятиях
	Итого	1		
Итого за семестр		18		
	Подготовка и сдача экзамена	36		Экзамен
Итого		72		

Согласована на портале № 47275

10. Курсовой проект / курсовая работа

Не предусмотрено РУП.

11. Рейтинговая система для оценки успеваемости обучающихся

11.1. Балльные оценки для элементов контроля

Таблица 11.1 – Балльные оценки для элементов контроля

Элементы учебной деятельности	Максимальный балл на 1-ую КТ с начала семестра	Максимальный балл за период между 1КТ и 2КТ	Максимальный балл за период между 2КТ и на конец семестра	Всего за семестр
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

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)

Согласована на портале № 47275

	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. Построение защищенных корпоративных сетей [Электронный ресурс] [Электронный ресурс]: учебное пособие / Р.Н. Ачилов. — Электрон. дан. — Москва : ДМК Пресс, 2013. — 250 с. — Режим доступа: https://e.lanbook.com/book/66472 (дата обращения: 19.05.2018).

12.2. Дополнительная литература

1. Компьютерные сети и службы удаленного доступа [Электронный ресурс] [Электронный ресурс]: справочник / О. Ибе. — Электрон. дан. — Москва : ДМК Пресс, 2007. — 336 с. — Режим доступа: https://e.lanbook.com/book/1169 (дата обращения: 19.05.2018).

12.3. Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Безопасность сетей ЭВМ [Электронный ресурс]: Методические указания для лабораторных и практических работ / Новохрестов А. К., Праскурин Г.А., 2014. – 99 с. [Электронный ресурс] — Режим доступа: http://kibevs.tusur.ru/sites/default/files/upload/work_progs/nak/BSEVM_lab_pract.pdf (дата обращения: 19.05.2018).
2. Безопасность сетей ЭВМ [Электронный ресурс]: Методические указания для самостоятельной работы студента / Новохрестов А.К., Праскурин Г.А., 2014. – 4 с. [Электронный ресурс] — Режим доступа: http://kibevs.tusur.ru/sites/default/files/upload/work_progs/nak/BSEVM_sam.pdf (дата обращения: 19.05.2018).
3. Безопасность сетей ЭВМ. Часть 1 [Электронный ресурс]: Лабораторный практикум / Новохрестов А. К., Гуляев А. И. - 2017. 92 с. — Режим доступа: https://edu.tusur.ru/publications/7225 (дата обращения: 19.05.2018).

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

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

Для лиц с нарушениями зрения:

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

Для лиц с нарушениями слуха:

- в форме электронного документа;
- в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

- в форме электронного документа;
- в печатной форме.

12.4. Профессиональные базы данных и информационные справочные системы

1. 1. http://www.elibrary.ru - научная электронная библиотека;
2. 2. http://www.edu.ru - веб-сайт системы федеральных образовательных порталов;
3. 3. http://edu.fb.tusur.ru/ - образовательный портал факультета безопасности;
4. 4. https://fstec.ru/ - Федеральная служба по техническому и экспортному контролю.

13. Материально-техническое обеспечение дисциплины и требуемое программное

Согласована на портале № 47275

обеспечение

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

13.1.1. Материально-техническое и программное обеспечение для лекционных занятий

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

13.1.2. Материально-техническое и программное обеспечение для практических занятий

Лаборатория безопасности сетей ЭВМ / Лаборатория криптографии в банковском деле

учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа

634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 804 ауд.

Описание имеющегося оборудования:

- Компьютеры класса не ниже GigaByte GA-F2A68HM-DS2 rev1.0 (RTL) / AMD A4-6300 / DDR-III DIMM 8Gb / SVGARadeon HD 8370D / HDD 1Tb Gb SATA-III Seagate (10 шт.);
- Обучающий стенд локальные компьютерные сети Microtik routerboard (2 шт.);
- ViPNET УМК «Безопасность сетей»;
- Коммутатор Mikrotik CRS125-24G-1S-IN (6 шт.);
- Компьютер класса не ниже i5-7400/8DDR4/SSD120G;
- Анализатор кабельных сетей MI 2016 Multi LAN 350 (3 шт.);
- Анализатор Wi-Fi сетей NETSCOUT AirCheck G2 (2 шт.);
- Сервер класса не ниже 4xE7-4809v4/512GBRE16/L9300-8i/5T6000G7;
- Маршрутизатор Cisco 891-K9 (2 шт.);
- Маршрутизатор Cisco C881-V-K9 (2 шт.);
- Маршрутизатор Check Point CPAP-SG1200R-NGFW (2 шт.);
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

- Cisco Packet Tracer
- Система мониторинга Zabbix
- Microsoft Windows 10
- XSpider
- Анализатор трафика Wireshark
- Дистрибутив Kali Linux
- Межсетевой экран ИКС Lite
- МежсетевойэкранPositive Technologies Application Firewall Education
- Система анализа защищенности сети MaxPatrol Education
- Система обнаружения вторжений Snort
- Система обнаружения вторжений Suricata
- Средство построения виртуальных частных сетей OpenVPN

13.1.3. Материально-техническое и программное обеспечение для лабораторных работ

Лаборатория программно-аппаратных средств обеспечения информационной безопасности

учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа

634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 405 ауд.

Описание имеющегося оборудования:

- Компьютеры класса не ниже M/B ASUSTeK S-775 P5B i965 / Core 2 Duo E6300 / DDR-II DIMM 2048 Mb / Sapphire PCI-E Radeon 256 Mb / 160 Gb Seagate (15 шт.);

Согласована на портале № 47275

- Комплект специализированной учебной мебели;
- Аппаратные средства аутентификации пользователя «eToken Pro»;
- Программно-аппаратный комплекс защиты информации: ПАК ViPNet Coordinator HW100 C 4.x, ПАК ViPNet Coordinator HW1000 4.x, ПАК Аккорд;
- Рабочее место преподавателя.

Стенды для изучения проводных и беспроводных компьютерных сетей, включающие:
- абоненские устройства: компьютеры SuperMicro;
- коммутаторы: Mikrotik CRS125-24G-1S-IN; Mikrotik RouterBoard 1100;
- маршрутизаторы: Cisco 891-K9, Cisco C881-V-K9, Check Point CPAP-SG1200R-NGFW;
- средства анализа сетевого трафика и углубленной проверки сетевых пакетов: анализатор трафика Wireshark, дистрибутив Kali Linux;
- межсетевые экраны: ИКС Lite, Positive Technologies Application Firewall Education, CISCO ASA 5505, МЭ в составе маршрутизатора Check Point CPAP-SG1200R-NGFW;
- системы обнаружения компьютерных атак: Snort, Suricata, СОВ в составе маршрутизатора Check Point CPAP-SG1200R-NGFW;
- точки доступа: D-link dwl3600ap;
- системы защиты от утечки данных: Контур информационной безопасности SearchInform;
- средства мониторинга состояния автоматизированных систем: система мониторинга Zabbix;
- средства сканирования защищенности компьютерных сетей: сканер безопасности Xspider Education, система анализа защищенности сети MaxPatrol Education;

Программное обеспечение:
– Антивирусный программный комплекс: Kaspersky endpoint security ;
– Microsoft Windows 7 Pro;
– VirtualBox;
– Криптографическое средство защиты информации КриптоПро CSP;
– Аппаратно-программные средства управления доступом к данным шифрования: ПО ViPNet Administrator 4.x, ПО ViPNet Coordinator for Windows 4.x, ПО ViPNet Coordinator for Linux 4.x, ПО ViPNet Client for Windows 4.x, ПО ViPNet Crypto Service 4.x, КриптоПро CSP, DallasLock;
– Visual Studio.

Лаборатория безопасности сетей ЭВМ / Лаборатория криптографии в банковском деле

учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа

634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 804 ауд.

Описание имеющегося оборудования:
- Компьютеры класса не ниже GigaByte GA-F2A68HM-DS2 rev1.0 (RTL) / AMD A4-6300 / DDR-III DIMM 8Gb / SVGARadeon HD 8370D / HDD 1Tb Gb SATA-III Seagate (10 шт.);
- Обучающий стенд локальные компьютерные сети Microtik routerboard (2 шт.);
- ViPNET УМК «Безопасность сетей»;
- Коммутатор Mikrotik CRS125-24G-1S-IN (6 шт.);
- Компьютер класса не ниже i5-7400/8DDR4/SSD120G;
- Анализатор кабельных сетей MI 2016 Multi LAN 350 (3 шт.);
- Анализатор Wi-Fi сетей NETSCOUT AirCheck G2 (2 шт.);
- Сервер класса не ниже 4xE7-4809v4/512GBRE16/L9300-8i/5T6000G7;
- Маршрутизатор Cisco 891-K9 (2 шт.);
- Маршрутизатор Cisco C881-V-K9 (2 шт.);
- Маршрутизатор Check Point CPAP-SG1200R-NGFW (2 шт.);
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:
– Cisco Packet Tracer
– Система мониторинга Zabbix
– Microsoft Windows 10

Согласована на портале № 47275

- XSpider
- Анализатор трафика Wireshark
- Дистрибутив Kali Linux
- Межсетевой экран ИКС Lite
- МежсетевойэкранPositive Technologies Application Firewall Education
- Система анализа защищенности сети MaxPatrol Education
- Система обнаружения вторжений Snort
- Система обнаружения вторжений Suricata
- Средство построения виртуальных частных сетей OpenVPN

13.1.4. Материально-техническое и программное обеспечение для самостоятельной работы

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

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

Состав оборудования:

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

Перечень программного обеспечения:

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

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

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

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

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

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

Согласована на портале № 47275

14. Оценочные материалы и методические рекомендации по организации изучения дисциплины

14.1. Содержание оценочных материалов и методические рекомендации

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

14.1.1. Тестовые задания

1. По масштабу компьютерные сети подразделяются на

a) звездообразные, кольцевые, шинные

b) одноранговые и сети "клиент-сервер"

c) проводные и беспроводные

d) локальные и глобальные

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

a) прикладного

b) сетевого

c) канального

d) физического

3. Какое минимальное количество уровней протоколов (в терминах модели OSI) должны поддерживать маршрутизаторы сетей с коммутацией пакетов?

a) 1

b) 2

c) 3

d) 4

4. К транспортному уровню модели OSI относятся протоколы:

a) IP, RIP, OSPF

b) SSL, TLS

c) SMTP, IMAP, POP3

d) UDP, TCP

5. По какой причине в протоколе RIP расстояние в 16 хопов между сетями полагается недостижимым?

a) поле, отведенное для хранения значения расстояния, имеет длину 4 двоичных разряда

b) для получения приемлемого времени сходимости алгоритма

c) сети, в которых работает RIP, редко бывают большими

d) таблицы маршрутизации не могут хранить больше 16 записей

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

a) создать диапазон IP адресов

b) создать параметр DHCP

c) создать область DHCP

d) создать исключение для IP адреса

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

a) сетевой доступ

b) каталог

c) папка

d) домен

8. Какой протокол используется для доступа к службе каталогов AD?

a) LDAP

b) ShareDiscovery

c) ADSL

d) UDP

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

a) хабом

Согласована на портале № 47275

b) сервером

c) рабочей станцией

d) хостом

10. Метод передачи данных, при котором данные пересылаются в двух направлениях одновременно, называется …

a) симплексным

b) дуплексным

c) синхронным

d) полудуплексным

11. Анализ защищенности - это …

a) выбор обоснованного набора контрмер, позволяющих снизить уровень рисков до приемлемой величины

b) независимая экспертиза отдельных областей функционирования предприятия

c) процедура учета действий, выполняемых пользователем на протяжении сеанса доступа

d) поиск уязвимых мест информационной системы

12. Воздействие на систему с целью создания условий, при которых легальные пользователи системы не могут получить доступ к предоставляемым системой ресурсам, либо этот доступ затруднен.

a) DoS-атака

b) несанкционированный доступ

c) незаконное использование привилегий

d) программная закладка

13. Программное средство для удаленной или локальной диагностики различных элементов сети на предмет выявления в них различных уязвимостей.

a) агент безопасности

b) политика безопасности

c) средство делегирования административных полномочий

d) сканер безопасности

14. … - процесс блокировки выявленных вторжений.

a) анализ защищенности

b) обнаружение атак

c) предотвращение атак

d) аудит безопасности

15. В журнале аутентификации обнаружено несколько записей неуспешных попыток войти в систему под учетными записями пользователей. Возможно была попытка подбора паролей. Какое стандартное средство следует использовать для уменьшения риска такого рода атак?

a) использовать систему обнаружения вторжений

b) переименовать учетную запись администратора

c) использовать мультифакторную аутентификацию

d) включить блокировку учетных записей при определенном количестве неуспешных попыток регистрации

16. Политика безопасности требует сокрытия схемы IP-адресации, используемой во внутренней сети. Какая из перечисленных технологий позволит решить поставленную задачу?

a) система обнаружения вторжений

b) персональный межсетевой экран

c) NAT

d) антивирусное программное обеспечение

17. Технология, которая для обнаружения атак использует, например, образец IP-пакета, характерного для какой-нибудь определенной атаки.

a) монитор регистрационных файлов

b) контроль целостности

c) выявление аномальной деятельности

d) анализ сигнатур

18. Согласно классификации ФСТЭК России, межсетевой экран применяемый на

Согласована на портале № 47275

логической границе ИС или между логическими границами сегментов ИС, это МЭ …

a) типа А

b) типа Б

c) типа В

d) типа Г

19. Согласно классификации ФСТЭК России системы обнаружения вторжений делятся на

a) уровня узла и уровня сети

b) внешние и внутренние

c) симметричные и асимметричные

d) коммутируемые и некоммутируемые

20. Согласно профилю защиты средства антивирусной защиты типа «Б» устанавливаются на … информационной системы, функционирующей на базе вычислительной сети.

a) рабочие станции пользователей

b) серверы

c) рабочую станцию администратора

d) серверы и рабочие станции

21. Защита ресурсов сети от несанкционированного использования - это

a) охрана оборудования сети

b) защита ядра безопасности

c) контроль доступа

d) защита периметра безопасности

22. Средство защиты, обеспечивающее защищенность информации от угроз нелегитимной передачи данных из защищенного сегмента системы путем анализа и блокирования исходящего трафика

a) межсетевой экран

b) средство антивирусной защиты

c) DLP-система

d) сканер безопасности

23. Средство, решающее задачи консолидации и хранения журналов событий от различных источников, а также имеющее инструменты для анализа событий и разбора инцидентов на основе их корреляции и обработки по правилам – это …

a) DLP-система

b) система обнаружения вторжений

c) SIEM-система

d) сканер безопасности

24. Способ перехвата информации, при котором на машину устанавливается программное средство, собирающее и передающее информацию – это …

a) перехват в разрыв

b) сетевой перехват

c) агентский перехват

d) перехват путем интеграции со сторонними продуктами

25. Программное или аппаратное средство, которое осуществляет мониторинг сети в реальном времени с целью выявления, предотвращения и блокировки вредоносной активности.

a) межсетевой экран

b) система обнаружения вторжений

c) система предотвращения вторжений

d) средство антивирусной защиты

26. К каким методам сбора данных, использующихся при аудите информационной безопасности, относится MaxPatrol?

a) анализ документации

b) предоставление опросных листов

c) использование специализированных программных средств

d) интервьюирование

27. Какой из методов проверки направлен на определение наличия уязвимости по

Согласована на портале № 47275

косвенным признакам?

a) активные зондирующие проверки

b) проверка заголовков и активные зондирующие проверки

c) проверка заголовков

d) имитация атак

28. В каком режиме сканирования системы анализа защищенности MaxPatrol можно произвести подбор паролей?

a) Audit

b) Compliance

c) PenTest

d) Pentest и Compliance

29. В каком режиме функционирования IPsec шифруется весь исходный IP-пакет, а затем он вставляется в поле данных нового пакета?

a) транспортном

b) туннельном

c) в обоих режимах

d) IPsec не использует шифрование

30. Процесс получения объективных качественных и количественных оценок о текущем состоянии информационной безопасности организации в соответствии с определёнными критериями и показателями безопасности – это …

a) выявление аномальной деятельности

b) анализ защищённости

c) аудит информационной безопасности

d) установка системы защиты

14.1.2. 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`у.

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.

Согласована на портале № 47275

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 прикладных сервисов (Веб, почта, FTP) и их решения.

30. Физические средства обеспечения информационной безопасности.

14.1.3. 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.

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

Согласована на портале № 47275

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.

14.1.4. 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

14.1.5. 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.

Согласована на портале № 47275

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.

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

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

Согласована на портале № 47275

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

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

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

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

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

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

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

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

Для лиц с нарушениями зрения:

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

Для лиц с нарушениями слуха:

- в форме электронного документа;
- в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

- в форме электронного документа;
- в печатной форме.

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

Согласована на портале № 47275