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

Документ подписан электронной подписью
Сертификат: 1c6cfa0a-52a6-4f49-aef0-5584d3fd4820
Владелец: Троян Павел Ефимович
Действителен: с 19.01.2016 по 16.09.2019

РАБОЧАЯ ПРОГРАММА Д

Безопасность вычислительных сетей

Уровень образования: **высшее образование - специалитет**
Направление подготовки / специальность: **38.05.01 Экономическая безопасность**
Специализация: **Экономико-правовое обеспечение экономической безопасности**
Направленность (профиль): **Регламентация работы персонала организации при обеспечении экономической и информационной безопасности**
Форма обучения: **заочная**
Факультет: **ЗиВФ, Заочный и вечерний факультет**
Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**
Курс: **4, 5**
Семестр: **8, 9**
Учебный план набора 2013 года

Распределение рабочего времени

№	Виды учебной деятельности	8 семестр	9 семестр	Всего	Единицы
1	Лекции	2	4	6	часов
2	Лабораторные работы	4	8	12	часов
3	Всего аудиторных занятий	6	12	18	часов
4	Из них в интерактивной форме	2	4	6	часов
5	Самостоятельная работа	66	56	122	часов
6	Всего (без экзамена)	72	68	140	часов
7	Подготовка и сдача зачета	0	4	4	часов
8	Общая трудоемкость	72	72	144	часов
				4.0	З.Е.

Контрольные работы: 9 семестр - 1
Зачет: 9 семестр

Томск 2018

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

ЛИСТ СОГЛАСОВАНИЯ

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

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 ЗиВФ _____ И. В. Осипов

Заведующий выпускающей каф. КИБЭВС _____ А. А. Шелупанов

Эксперты:

доцент каф. КИБЭВС _____ Е. Ю. Костюченко

доцент каф. КИБЭВС _____ К. С. Сарин

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 вычислительных сетей» (Б1.В.ДВ.5.1) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Информатика, Безопасность вычислительных сетей.

Последующими дисциплинами являются: Управление информационной безопасностью, Безопасность вычислительных сетей.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- ПК-20 способностью соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности;

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.

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 4.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры	
		8 семестр	9 семестр
Аудиторные занятия (всего)	18	6	12

Лекции	6	2	4
Лабораторные работы	12	4	8
Из них в интерактивной форме	6	2	4
Самостоятельная работа (всего)	122	66	56
Подготовка к контрольным работам	42	42	0
Оформление отчетов по лабораторным работам	48	16	32
Проработка лекционного материала	24	8	16
Выполнение контрольных работ	8	0	8
Всего (без экзамена)	140	72	68
Подготовка и сдача зачета	4	0	4
Общая трудоемкость, ч	144	72	72
Зачетные Единицы	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	Лаб. раб., ч	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
8 семестр					
1 Основные понятия информационных сетей	1	0	24	25	ПК-20
2 Основы построения современных локальных сетей	1	4	42	47	
Итого за семестр	2	4	66	72	
9 семестр					
3 Технологии обеспечения безопасности в локальных сетях	1	2	12	15	ПК-20
4 Обеспечение безопасности межсетевого взаимодействия	3	6	44	53	ПК-20
Итого за семестр	4	8	56	68	
Итого	6	12	122	140	

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.	1	ПК-20
	Итого	1	
2 Основы построения современных 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.	1	ПК-20
	Итого	1	
Итого за семестр		2	
9 семестр			
3 Технологии обеспечения безопасности в локальных сетях	Типовые угрозы сетевой безопасности. Основы классификации сетевых угроз и атак. Регламентирующие документы в области безопасности вычислительных сетей. Стандарты безопасности вычислительных сетей и их компонентов. Правовые основы защиты информации в сетях.	1	ПК-20
	Итого	1	
4 Обеспечение безопасности межсетевого взаимодействия	Основные механизмы обеспечения безопасности и управления распределенными ресурсами. Обеспечение надежности инфраструктуры Интернет.	1	ПК-20
	Защита каналов связи в Интернет. Виды используемых в Интернет каналов связи. Использование межсетевых экранов. Виртуальные частные сети.	1	
	Уязвимости и защита базовых протоколов и служб: Протоколы маршрутизации. Семейство TCP/IP. Службы поиска. Безопасность WWW и электронной почты.	1	
	Итого	3	
Итого за семестр		4	
Итого		6	

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

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.	Лаб. раб.	Сам. раб.	
ПК-20	+	+	+	Контрольная работа, Отчет по лабораторной работе, Опрос на занятиях, Зачет, 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	Всего, ч
8 семестр			
IT-методы	2		2
Итого за семестр:	2	0	2
9 семестр			
Презентации с использованием слайдов с обсуждением		2	2
IT-методы	2		2
Итого за семестр:	2	2	4
Итого	4	2	6

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
8 семестр			
2 Основы построения современных локальных сетей	Настройка подключения узла к сети. Автоматическая динамическая и статическая настройки сетевого подключения.	1	ПК-20
	Стек протоколов TCP/IP. Прикладные протоколы сети Интернет.	1	
	Сети Microsoft Windows. Управление сетевыми ресурсами в одноранговой сети.	1	
	Сети Microsoft Windows. Управление сетевыми ресурсами в выделенным сервером.	1	
	Итого	4	

Итого за семестр		4	
9 семестр			
3 Технологии обеспечения безопасности в локальных сетях	Инструменты для исследования сети (сниферы)	1	ПК-20
	Инструменты для исследования сети (сканеры безопасности)	1	
	Итого	2	
4 Обеспечение безопасности межсетевого взаимодействия	Межсетевые экраны	1	ПК-20
	Антивирусная защита	1	
	Виртуальные частные сети	1	
	Системы обнаружения и предотвращения вторжений	1	
	DLP-системы	1	
	Безопасность прикладных протоколов	1	
	Итого	6	
Итого за семестр		8	
Итого		12	

8. Практические занятия (семинары)

Не предусмотрено РУП.

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	Проработка лекционного материала	4	ПК-20	Зачет, Контрольная работа, Опрос на занятиях, Тест
	Подготовка к контрольным работам	20		
	Итого	24		
2 Основы построения современных локальных сетей	Проработка лекционного материала	4	ПК-20	Контрольная работа, Опрос на занятиях, Отчет по лабораторной работе, Тест
	Оформление отчетов по лабораторным работам	16		
	Подготовка к контрольным работам	22		
	Итого	42		
Итого за семестр		66		
9 семестр				
3 Технологии	Проработка лекционного	4	ПК-20	Опрос на занятиях, От-

обеспечения безопасности в локальных сетях	материала			чет по лабораторной работе, Тест
	Оформление отчетов по лабораторным работам	8		
	Итого	12		
4 Обеспечение безопасности межсетевого взаимодействия	Выполнение контрольных работ	8	ПК-20	Контрольная работа, Опрос на занятиях, Отчет по лабораторной работе, Тест
	Проработка лекционного материала	12		
	Оформление отчетов по лабораторным работам	24		
	Итого	44		
Итого за семестр		56		
	Подготовка и сдача зачета	4		Зачет
Итого		126		

10. Курсовой проект / курсовая работа

Не предусмотрено РУП.

11. Рейтинговая система для оценки успеваемости обучающихся

Рейтинговая система не используется.

12. Учебно-методическое и информационное обеспечение дисциплины

12.1. Основная литература

1. Построение защищенных корпоративных сетей [Электронный ресурс] : учебное пособие / Р.Н. Ачилов. — Электрон. дан. — Москва : ДМК Пресс, 2013. — 250 с. [Электронный ресурс] - Режим доступа: https://e.lanbook.com/book/66472 (дата обращения: 26.06.2018).

12.2. Дополнительная литература

1. Компьютерные сети и службы удаленного доступа [Электронный ресурс] : справочник / О. Ибе. — Электрон. дан. — Москва : ДМК Пресс, 2007. — 336 с. [Электронный ресурс] - Режим доступа: https://e.lanbook.com/book/1169 (дата обращения: 26.06.2018).

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] - Режим доступа: http://kibevs.tusur.ru/sites/default/files/upload/work_progs/nak/BSEVM_lab_pract.pdf (дата обращения: 26.06.2018).

2. Безопасность сетей ЭВМ: 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: 26.06.2018).

3. Безопасность сетей ЭВМ. Часть 1: Лабораторный практикум / Новохрестов А. К., Гуляев А. И. - 2017. 92 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/7225 (дата обращения: 26.06.2018).

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

13. Материально-техническое обеспечение дисциплины и требуемое программное обеспечение

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

13.1.1. Материально-техническое и программное обеспечение для лекционных занятий

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

13.1.2. Материально-техническое и программное обеспечение для лабораторных работ

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:

- Компьютер: DEPO Neos DF226/ i3-7100/ DDR4 8G/ Жесткий диск 500G/ мышь/ клавиатура/ монитор (14 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 самостоятельной работы

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

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

Состав оборудования:

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

Перечень программного обеспечения:

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

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

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

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

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

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

14. Оценочные материалы и методические рекомендации по организации изучения дисциплины

14.1. Содержание оценочных материалов и методические рекомендации

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

14.1.1. Тестовые задания

1. По масштабу компьютерные сети подразделяются на

a) звездообразные, кольцевые, шинные
b) одноранговые и сети "клиент-сервер"
c) проводные и беспроводные
d) локальные и глобальные

2. 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
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 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

14.1.2. 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.

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.

Типовые угрозы сетевой безопасности. Основы классификации сетевых угроз и атак. Регламентирующие документы в области безопасности вычислительных сетей. Стандарты безопасности вычислительных сетей и их компонентов. Правовые основы защиты информации в сетях.

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.

14.1.3. Зачёт

1. Понятие сети. Требования, предъявляемые к сети. 2. Классификация сетей. Признаки классификации. 3. Сетевые топологии. Преимущества и недостатки базовых сетевых топологий. 4. Методы коммутации узлов сети. Преимущества и недостатки различных методов коммутации. 5. Методы адресации в малых и больших сетях. Требования к адресам. 6. Основные аппаратные и программные компоненты компьютерных сетей 7. Назначение и состав линий связи. Назначение каждого компонента линий связи. 8. Основные виды передающих сред. Их характеристики. Ограничения передающих сред. 9. Беспроводная линия связи. Состав оборудования. Понятие канала. 10. Сетевая модель OSI. Назначение. Уровни взаимодействия открытых систем. 11. Стандартизация сетей. Проект 802.x. 12. Методы доступа к среде передачи данных. 13. Понятие протокола и интерфейса. Стеки протоколов. Стандартные стеки протоколов. 14. Сетевая архитектура Ethernet. Базовый стандарт. Компоненты реализации на физическом уровне. 15. Структура кадра технологии Ethernet. Технология VLAN. Стандарт IEEE 802.1q. 16. Сетевая архитектура Token Ring. 17. Сетевая архитектура FDDI. 18. Оборудование ЛВС. Принципы работы концентраторов, мостов, коммутаторов. 19. Сетевые операционные системы. Требования, предъявляемые к сетевым ОС. 20. Базовые примитивы передачи сообщений в распределенной сети. Вызов удаленных процедур. Механизм сокетов. 21. Сетевые файловые системы. Семантика разделения файлов. 22. Службы именования ресурсов. Служба каталогов. Доменный подход. 23. Служба каталогов Active Directory. Управление объектами сети. Групповые политики. 24. Задачи построения объединенных сетей. 25. Глобальная сеть Интернет. Построение. Основные понятия. Семейство протоколов TCP/IP и его роль в построении глобальных сетей. 26. Стек протоколов TCP/IP. Область применения. Основные характеристики. 27. Типы адресов, применяемых в сети Интернет. Назначение. Технологии разрешения адресов. 28. IP-адреса. Классы IP-сетей. 29. IP-адреса. Технология CIDR. Понятие сетевого префикса. 30. Оборудование ГВС. Краткая характеристика и назначение. 31. Структура сети Интернет. Автономные системы и Магистральные сети. Типы протоколов маршрутизации. 32. Маршрутизация IP-протокола. Алгоритмы маршрутизации. 33. Протоколы маршрутизации RIP и OSPF. Характеристики, достоинства и недостатки. 34. Протокол ARP. Назначение. Принцип функциони-

рования. 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.

14.1.4. Темы контрольных работ

Основные понятия информационных сетей

Основы построения современных локальных сетей

Технологии обеспечения безопасности в локальных сетях

Обеспечение безопасности межсетевого взаимодействия

14.1.5. 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)

Антивирусная защита

Виртуальные частные сети

Системы обнаружения и предотвращения вторжений

DLP-системы

Безопасность прикладных протоколов

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

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

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

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

показаниям	контрольные работы, устные ответы	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.