МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

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

УТВЕРЖДАЮ
Проректор по учебной работе
_____ П. В. Сенченко
«___» _____ 20__ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Защита информации в системах беспроводной связи

Уровень образования: **высшее образование - специалитет**
Направление подготовки / специальность: **10.05.02 Информационная безопасность телекоммуникационных систем**
Направленность (профиль) / специализация: **Защита информации в системах связи и управления**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **БИС, Кафедра безопасности информационных систем**
Курс: **5**
Семестр: **10**
Учебный план набора 2020 года

Распределение рабочего времени

№	Виды учебной деятельности	10 семестр	Всего	Единицы
1	Лекции	18	18	часов
2	Лабораторные работы	36	36	часов
3	Всего аудиторных занятий	54	54	часов
4	Самостоятельная работа	54	54	часов
5	Всего (без экзамена)	108	108	часов
6	Общая трудоемкость	108	108	часов
		3.0	3.0	З.Е.

Зачёт: 10 семестр

Томск

ЛИСТ СОГЛАСОВАНИЯ

Рабочая программа дисциплины составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 10.05.02 Информационная безопасность телекоммуникационных систем, утвержденного 16.11.2016 года, рассмотрена и одобрена на заседании кафедры БИС «___» _____ 20__ года, протокол №_____.

Разработчики:

Профессор каф. КИБЭВС _____ В. С. Аврамчук

Преподаватель каф. КИБЭВС _____ В. А. Фаерман

Заведующий обеспечивающей каф. БИС _____ Е. Ю. Костюченко

Рабочая программа дисциплины согласована с факультетом и выпускающей кафедрой:

Декан ФБ _____ Д. В. Кручинин

Заведующий выпускающей каф. БИС _____ Е. Ю. Костюченко

Эксперты:

Доцент кафедры комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) _____ А. А. Конев

Доцент кафедры комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) _____ К. С. Сарин

1. Цели и задачи дисциплины

1.1. Цели дисциплины

Обучить студентов основам построения и эксплуатации распределенных автоматизированных систем, использующих беспроводные каналы передачи данных, принципам и методам защиты информации в подобных системах, навыкам комплексного проектирования, построения и анализа защищенных систем беспроводной связи.

1.2. Задачи дисциплины

- – изучение технологий и протоколов беспроводной передачи данных;
- – рассмотрение архитектуры и классификации распределенных систем беспроводной связи;
- – выделение основных угроз информации в системах беспроводной связи;
- – изучение программно-аппаратных средств обеспечения безопасности в системах беспроводной связи.

2. Место дисциплины в структуре ОПОП

Дисциплина «Защита информации в системах беспроводной связи» (Б1.Б.08.07) относится к блоку 1 (базовая часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Аппаратные средства телекоммуникационных систем, Безопасность сетевых протоколов низкого уровня, Моделирование систем и сетей телекоммуникаций, Программно-аппаратные средства обеспечения информационной безопасности, Управление информационной безопасностью телекоммуникационных систем.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- ПСК-10.4 способностью применять наиболее эффективные методы и средства для закрытия возможных каналов перехвата акустической речевой информации;
- ПСК-10.3 способностью оценивать возможности средств технических разведок в отношении к системам связи, управления и объектам информатизации;
- ПСК-10.2 способностью формировать технические задания и участвовать в разработке аппаратных и программных средств защиты информационно-телекоммуникационных систем;

В результате изучения дисциплины обучающийся должен:

- **знать** технологии беспроводной передачи данных; 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 беспроводных сетях передачи данных; 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 3.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры

		10 семестр
Аудиторные занятия (всего)	54	54
Лекции	18	18
Лабораторные работы	36	36
Самостоятельная работа (всего)	54	54
Оформление отчетов по лабораторным работам	30	30
Проработка лекционного материала	24	24
Всего (без экзамена)	108	108
Общая трудоемкость, ч	108	108
Зачетные Единицы	3.0	3.0

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
10 семестр					
1 Основы и особенности беспроводных технологий	2	2	4	8	ПСК-10.2, ПСК-10.3, ПСК-10.4
2 Принципы передачи информации в радиоэфире	4	4	4	12	ПСК-10.2, ПСК-10.3, ПСК-10.4
3 Виды беспроводных сетей. Основные угрозы информационной безопасности	4	10	12	26	ПСК-10.2, ПСК-10.3, ПСК-10.4
4 Построение защищенных распределенных систем на основе беспроводных сетей	4	12	20	36	ПСК-10.2, ПСК-10.4
5 Методика испытаний систем беспроводной связи	4	8	14	26	ПСК-10.2, ПСК-10.3
Итого за семестр	18	36	54	108	
Итого	18	36	54	108	

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
10 семестр			
1 Основы и особенности беспроводных	История развития беспроводной связи. Отличия проводных и беспроводных технологий передачи данных.Классификация	2	ПСК-10.3

технологий	беспроводных технологий по дальности действия, по топологии, по области действия.		
	Итого	2	
2 Принципы передачи информации в радиоэфире	Пакетная и синхронная передача в радиоэфире. Методы модуляции и технологии передачи. Методы доступа к среде. Методы широкополосной передачи сигнала.	4	ПСК-10.3, ПСК-10.4
	Итого	4	
3 Виды беспроводных сетей. Основные угрозы информационной безопасности	Классификация беспроводных сетей. Подслушивание. Отказ в обслуживании. Глушение клиентской станции. Глушение базовой станции. Угрозы криптозащиты.	4	ПСК-10.2, ПСК-10.3
	Итого	4	
4 Построение защищенных распределенных систем на основе беспроводных сетей	Специфика частотного регулирования. Основные принципы проектирования защищенных беспроводных сетей. Создание аутентификационной инфраструктуры. Применение криптографических алгоритмов. Применение инфраструктуры открытых ключей (PKI).	4	ПСК-10.2, ПСК-10.4
	Итого	4	
5 Методика испытаний систем беспроводной связи	Факторы, определяющие реальную производительность системы при беспроводной передаче данных. Рекомендуемый комплекс полевых испытаний. Образцовые тесты и результаты лабораторных испытаний. Методика тестирования оценки уровня защищенности.	4	ПСК-10.2, ПСК-10.3
	Итого	4	
Итого за семестр		18	

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
Предшествующие дисциплины					
1 Аппаратные средства телекоммуникационных систем	+	+		+	
2 Безопасность сетевых протоколов низкого уровня		+	+		
3 Моделирование систем и сетей телекоммуникаций				+	

4 Программно-аппаратные средства обеспечения информационной безопасности			+	+	
5 Управление информационной безопасностью телекоммуникационных систем				+	

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.	
ПСК-10.4	+	+	+	Контрольная работа, Отчет по лабораторной работе, Опрос на занятиях, Тест
ПСК-10.3	+	+	+	Контрольная работа, Отчет по лабораторной работе, Опрос на занятиях, Зачёт, Тест
ПСК-10.2	+	+	+	Контрольная работа, Отчет по лабораторной работе, Опрос на занятиях, Зачёт, Тест

6. Интерактивные методы и формы организации обучения

Не предусмотрено РУП.

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
10 семестр			
1 Основы и особенности беспроводных технологий	Запуск WLAN сети в инфраструктурном режиме. Настройка оборудования и режима работа.	2	ПСК-10.2
	Итого	2	
2 Принципы передачи информации в радиоэфире	Исследование трафика в WLAN сети. Взаимное обнаружение устройств. Структура кадров.	4	ПСК-10.2
	Итого	4	
3 Виды беспроводных сетей. Основные угрозы информационной безопасности	Штатные средства обеспечения безопасности беспроводных сетей. Шифрование. Фильтрация по MAC.	2	ПСК-10.4
	Средства тестирования безопасности беспроводных сетей на платформе Kali Linux. Базовый набор инструментов. Настройка рабочего режима.	4	
	Угроза типа «Отказ в обслуживание». Утилита MDK. Типовые атаки и способы защиты.	4	

	Итого	10	
4 Построение защищенных распределенных систем на основе беспроводных сетей	Криптозащита в системах беспроводной связи. Уязвимости протокола WEP. Утилита aircrack-ng.	4	ПСК-10.2, ПСК-10.4
	Современные технологии безопасности WLAN (WPA, WPA2). PSK-аутентификация. Словарные атаки. Утилиты Crunch, RainbowCrack, hashcat.	4	
	Протокол упрощённой настройки WPS. Варианты реализации и уязвимости. Утилиты Wash, Reaver, Pyrit.	4	
	Итого	12	
5 Методика испытаний систем беспроводной связи	Проведение аудита защищенности WLAN сетей. Утилиты WiFite, Fern.	8	ПСК-10.2, ПСК-10.3
	Итого	8	
Итого за семестр		36	

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
10 семестр				
1 Основы и особенности беспроводных технологий	Проработка лекционного материала	2	ПСК-10.3, ПСК-10.4	Тест
	Оформление отчетов по лабораторным работам	2		
	Итого	4		
2 Принципы передачи информации в радиоэфире	Проработка лекционного материала	2	ПСК-10.3, ПСК-10.4, ПСК-10.2	Опрос на занятиях, Отчет по лабораторной работе, Тест
	Оформление отчетов по лабораторным работам	2		
	Итого	4		
3 Виды беспроводных сетей. Основные угрозы информационной безопасности	Проработка лекционного материала	4	ПСК-10.2, ПСК-10.3, ПСК-10.4	Опрос на занятиях, Отчет по лабораторной работе, Тест
	Оформление отчетов по лабораторным работам	8		
	Итого	12		
4 Построение защищенных распределенных систем на основе	Проработка лекционного материала	8	ПСК-10.2, ПСК-10.4	Опрос на занятиях, Отчет по лабораторной работе, Тест
	Оформление отчетов по лабораторным работам	12		

беспроводных сетей	Итого	20		
5 Методика испытаний систем беспроводной связи	Проработка лекционного материала	8	ПСК-10.2, ПСК-10.3	Контрольная работа, Опрос на занятиях, Отчет по лабораторной работе, Тест
	Оформление отчетов по лабораторным работам	6		
	Итого	14		
Итого за семестр		54		
Итого		54		

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
10 семестр				
Зачёт	5	10	10	25
Контрольная работа	5	10	5	20
Опрос на занятиях	2	4	3	9
Отчет по лабораторной работе	8	8	10	26
Тест	5	10	5	20
Итого максимум за период	25	42	33	100
Нарастающим итогом	25	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.

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. Максим, М. Безопасность беспроводных сетей / М. Максим, Д. Поллино. — Москва [Электронный ресурс]: ДМК Пресс, 2008. — 288 с. — ISBN 5-94074-248-3. — Текст : электронный // Лань : электронно-библиотечная система. — Режим доступа: https://e.lanbook.com/book/1115 (дата обращения: 19.02.2021).

12.2. Дополнительная литература

1. Барнс, К. Защита от хакеров беспроводных сетей [Электронный ресурс] / К. Барнс, Т. Боутс, Д. Лойд, Э. Уле. — Электрон. дан. — Москва [Электронный ресурс] [Электронный ресурс]: ДМК Пресс, 2005. — 480 с. — Режим доступа: https://e.lanbook.com/book/1119 (дата обращения: 19.02.2021).
2. Защита информации в инфокоммуникационных системах и сетях [Электронный ресурс]: Учебное пособие / А. М. Голиков - 2015. 284 с. — Режим доступа: https://edu.tusur.ru/publications/5262 (дата обращения: 19.02.2021).

12.3. Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Исхаков А.Ю. Защита информации в системах беспроводной связи [Электронный ресурс] [Электронный ресурс]: методические указания для выполнения практических и самостоятельных работ [Электронный ресурс]. — Режим доступа: http://kibevs.tusur.ru/sites/default/files/upload/work_progs/iay/iskhakov_prot_wireless.zip. (дата обращения: 19.05.2018). — Режим доступа: http://kibevs.tusur.ru/sites/default/files/upload/work_progs/iay/iskhakov_prot_wireless.zip (дата обращения: 19.02.2021).
2. Исхаков А.Ю. Защита информации в системах беспроводной связи [Электронный ресурс] [Электронный ресурс]: методические указания для выполнения лабораторных работ для студентов специальности 10.05.02 "Информационная безопасность телекоммуникационных систем" [Электронный ресурс]. — Режим доступа: http://kibevs.tusur.ru/sites/default/files/upload/work_progs/iay/iskhakov_networks_lab.zip. — Режим доступа: http://kibevs.tusur.ru/sites/default/files/upload/work_progs/iay/iskhakov_networks_lab.zip (дата обращения: 19.02.2021).

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.iqlib.ru - электронная интернет библиотека.
2. http://www.biblioclub.ru – полнотекстовая электронная библиотека.
3. http://www.elibrary.ru - научная электронная библиотека.
4. http://www.edu.ru - веб-сайт системы федеральных образовательных порталов.
5. http://www.sec.ru – каталог организаций в сфере информационной безопасности.

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.);

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.

Стенды для изучения средств криптографической защиты информации в банковском деле, 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 криптографической защиты информации: программно-аппаратный комплекс шифрования «ФПСУ-IP», программно-аппаратный комплекс шифрования «ФПСУ-IP/Клиент»;
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

- Система мониторинга Zabbix
- Kaspersky endpoint security
- XSpider
- Анализатор трафика Wireshark
- МежсетевойэкранPositive Technologies Application Firewall Education
- Система анализа защищенности сети MaxPatrol Education
- Система обнаружения вторжений Snort
- Система обнаружения вторжений Suricata

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

Тест 1. Экранирование может использоваться для:
a. Анализа рисков.
b. Предупреждения нарушений информационной безопасности.
c. Обнаружения нарушений.
d. Локализации последствий нарушений.
Ответ____

Тест 2. Взаимное увеличение или уменьшение результирующей амплитуды двух или нескольких
когерентных волн при их наложении друг на друга называется …
a. Резонанс.
b. Интерференция.
c. Эффект «бегущей волны».
d. Эффект «стоячей волны».
Ответ____

Тест 3. В качестве аутентификатора в сетевой среде могут использоваться:
a. Клавиатурный почерк.
b. Номер карточки пенсионного страхования.
c. Результат работы генератора одноразовых паролей.
d. PIN-код.
Ответ____

Тест 4. Набор норм, правил и практических приемов, регулирующих управление, защиту и распространение ценной информации, называется …
a. Моделью безопасности.
b. Методом шифрования.
c. Компьютерной безопасностью.
d. Политикой безопасности.
Ответ____

Тест 5. Криптография необходима для реализации следующих сервисов безопасности:
a. Идентификация.
b. Экранирование.
c. Аудит.
d. Аутентификация.
Ответ____

Тест 6. Сколько уровней содержит модель взаимодействия открытых систем (OSI) ?
a. 3.
b. 7.

c. 10.
d. 32.
Ответ____

Тест 7. Какая международная организация отвечает за выделение уникальных глобальных адресов в сети Internet?
a. IEEE.
b. ISO.
c. FDDI.
d. ICANN.
Ответ____

Тест 8. Что из перечисленного может быть MAC-адресом?
a. 22:16:98:15.
b. 00:1B:12:86:E4:22.
c. 00:B0:A1:8C:32:65:BB.
d. 01:23:44:55:E4:6T.
Ответ____

Тест 9. Как принято называть блок данных формируемых протоколом IP?
a. Траффик.
b. Бит.
c. Пакет.
d. Кадр.
Ответ____

Тест 10. Token Ring – это…
a. Сетевая модель.
b. Сетевая архитектура.
c. Протокол канального уровня.
d. Протокол прикладного уровня.
Ответ____

Тест 11. Протоколирование и аудит могут использоваться для:
a. Обеспечения целостности информации.
b. Предупреждения нарушений информационной безопасности.
c. Реализации правил разграничения доступа.
d. Восстановления режима информационной безопасности.
Ответ____

Тест 12. Какая из особенностей не характерна для акустоэлектрического канала утечки информации ?
a. Отсутствие проблем с питанием у микрофона.
b. Возможность съёма информации с питающей сети без подключения к ней (используя электромагнитное излучение сети электропитания).
c. Возможные помехи на бытовых приборах при использовании электросети для передачи информации, а также плохое качество передаваемого сигнала при большом количестве работы бытовых приборов.
d. Несостоятельность как канала утечки информации в современном мире, обусловленная его недостаточным распространением.
Ответ____

Тест 13. Под определение средств защиты информации, данное в Законе «О государственной тайне», не подпадают:

a. Средства выявления злоумышленной активности.
b. Технические и программные средства защиты информации.
c. Средства контроля эффективности защиты информации.
d. Криптографические средства защиты.
Ответ____

Тест 14. Аутентификация на основе пароля, переданного по сети в зашифрованном виде с использованием сеансового ключа, не обеспечивает защиты от:
a. Перехвата.
b. Несанкционированного доступа.
c. Воспроизведения.
d. Атак на доступность.
Ответ____

Тест 15. Риск информационной безопасности – это…
a. Число уязвимостей в системе.
b. Отношение стоимости системы защиты к вероятности её «простоя».
c. Сочетание вероятности угрозы информационной безопасности и последствий её наступления.
d. Оценка стоимости защитных средств.
Ответ____

Тест 16. Отношение разности между максимальным и минимальным значениями амплитуд модулированного сигнала к сумме этих значений, выраженное в процентах
a. Джиттер.
b. Коэффициент модуляции.
c. Девиация.
d. Ширина спектра.
Ответ____

Тест 17. Что можно отнести к преимуществам частотной модуляции по сравнению с амплитудной модуляцией?
a. Больший радиус действия.
b. Неизменность исходного спектра.
c. Помехоустойчивость.
d. Отсутствие несущей частоты.
Ответ____

Тест 18. Каковы основные функции роли "аутентификатор (Authenticator)" согласно стандарту
IEEE 802.1X:
a. Управляет физическим доступом к сети, основываясь на статусе аутентификации клиента.
b. Запрашивает доступ к беспроводной локальной сети и отвечает на запросы точки доступа.
c. Выполняет фактическую аутентификацию клиента: проверяет подлинность клиента и информирует точку доступа о предоставлении или отказе клиенту в доступе к сети.
d. Инициирует процесс аутентификации.
Ответ____

Тест 19. Какая из перечисленных технологий не относится к классу WPAN?
a. ZigBee.
b. Bluetooth.
c. UWB.

d. UMTS.
Ответ____

Тест 20. Разновидность сетевой атаки типа MITM (Man in the middle), применяемая в сетях с
использованием протокола ARP
a. "ARP-spoofing".
b. "Negative ARP".
c. IPSEC.
d. VLAN-ARP.
Ответ____

Тест 21. Политика безопасности строится на основе:
a. Общих представлений об информационной системе организации.
b. Изучения политик родственных организаций.
c. Количества рабочих станций.
d. Анализа рисков.
Ответ____

Тест 22. Каким принципом следует руководствоваться для обеспечения информационной безопасности сетевых конфигураций?
a. Выработка и проведение в жизнь единой политики безопасности.
b. Унификация аппаратно-программных платформ.
c. Увеличение затрат на средства защиты.
d. Минимизация числа используемых приложений.
Ответ____

Тест 23. Криптография необходима для реализации следующих сервисов безопасности:
a. Контроль конфиденциальности.
b. Контроль вторжений.
c. Контроль доступности.
d. Контроль непротиворечивости.
Ответ____

Тест 24. Выберите неверное утверждение. Сигнатурный метод выявления атак характеризуется:
a. Сравнением исследуемого объекта с ранее известными образцами-эталонами.
b. Способностью обнаруживать ранее неизвестные атаки.
c. Простотой в настройке и эксплуатации для конечного пользователя системы.
d. Популярностью использования в системах антивирусной защиты.
Ответ____

Тест 25. Устройство, предназначенное для защиты помещений от утечки информации по акустическим и виброканалам и специально разработанное для сеансового блокирования подслушивающих устройств, называется ?
a. Модулятор.
b. Колонка зашумления.
c. Генератор виброакустического шума.
d. Синтезатор шума.
Ответ____

Тест 26. Программно-аппаратный элемент компьютерной сети, осуществляющий контроль и
фильтрацию проходящего через него сетевого трафика в соответствии с заданными прави-

лами, – это …

a. Межсетевой экран.
b. Коммутатор.
c. Блокирующий маршрутизатор.
d. Шлюз сеансового уровня.
Ответ____

Тест 27. Пакетные фильтры функционируют
a. На канальном уровне.
b. На прикладном уровне.
c. На физическом уровне.
d. На сетевом уровне.
Ответ____

Тест 28. В графе структуры сети рангом пути называется
a. Общее число путей между заданными узлами.
b. Число узлов, входящих в данный путь.
c. Минимальное число независимых путей.
d. Число ребер, входящих в данный путь.
Ответ____

Тест 29. Превышение максимальной мощности сигнала средней мощности – это…
a. Емкость сигнала.
b. Пик-фактор.
c. Объем сигнала.
d. Представляющий (информационный) параметр.
Ответ____

Тест 30. Условие возникновения эффекта «перемодуляци»:
a. Коэффициент модуляции <1.
b. Коэффициент модуляции >1.
c. Коэффициент модуляции =1.
d. Коэффициент модуляции <0,5.
Ответ____

14.1.2. Темы опросов на занятиях

История развития беспроводной связи. Отличия проводных и беспроводных технологий передачи данных.Классификация беспроводных технологий по дальности действия, по топологии, по области действия.

Пакетная и синхронная передача в радиоэфире. Методы модуляции и технологии передачи. Методы доступа к среде. Методы широкополосной передачи сигнала.

Классификация беспроводных сетей. Подслушивание. Отказ в обслуживании. Глушение клиентской станции. Глушение базовой станции. Угрозы криптозащиты.

Специфика частотного регулирования. Основные принципы проектирования защищенных беспроводных сетей. Создание аутентификационной инфраструктуры. Применение криптографических алгоритмов. Применение инфраструктуры открытых ключей (PKI).

Факторы, определяющие реальную производительность системы при беспроводной передаче данных. Рекомендуемый комплекс полевых испытаний. Образцовые тесты и результаты лабораторных испытаний. Методика тестирования оценки уровня защищенности.

14.1.3. Зачёт

1. Что стандартизирует модель OSI?

2. Можно ли представить еще один вариант модели взаимодействия открытых систем с другим количеством уровней, например 8 или 5?

3. Ниже перечислены оригинальные (англоязычные) названия семи уровней модели OSI. Отметьте, какие из названий уровней не соответствуют стандарту?

physical layer, data-link layer, network layer, transport layer, seances layer, presentation layer, application layer.

4. Какие из приведенных утверждений вы считаете ошибочными:

– протокол – это программный модуль, решающий задачу взаимодействия систем;

– протокол – это формализованное описание правил взаимодействия, включающих последовательность обмена сообщениями и их форматы;

– термины «интерфейс» и «протокол», в сущности, являются синонимами.

5. На каком уровне модели OSI работает прикладная программа?

6. Как вы считаете, протоколы транспортного уровня устанавливаются только на конечных узлах, только на промежуточном коммуникационном оборудовании (маршрутизаторах) или и там, и там?

7. На каком уровне модели OSI работают сетевые службы?

8. Ниже перечислены некоторые сетевые устройства:

– маршрутизатор;

– коммутатор;

– мост;

– повторитель;

– сетевой адаптер;

– концентратор.

В каком из этих устройств реализуются функции физического уровня модели OSI? Канального уровня? Сетевого уровня?

9. Какое название традиционно используется для единицы передаваемых данных на каждом из уровней OSI?

10. Дайте определение открытой системы.

11. Пусть малоизвестная небольшая компания предлагает нужный вам продукт с характеристиками, превосходящими характеристики аналогичных продуктов известных фирм. В каком из перечисленных вариантов ваши действия можно считать согласующимися с принципом открытых систем:

– приму предложение, проверив прилагаемую документацию и убедившись, что в ней указаны характеристики, превосходящие известные аналоги;

– приму предложение только после того, как проведу тестирование и удостоверюсь, что характеристики действительно лучше;

– в любом случае откажусь в пользу продукта известной фирмы, так как последняя наверняка следует стандартам, а значит, будет меньше проблем с совместимостью;

– откажусь от продукта неизвестной компании, так как есть риск ее исчезновения, а значит, могут быть проблемы с поддержкой.

12. Какая организация разработала стандарты сетей Ethernet?

13. Какое из административных подразделений Интернета непосредственно занимается стандартизацией?

14. Какие из перечисленных терминов являются синонимами:

– стандарт;

– спецификация;

– RFC;

– никакие.

15. К какому типу стандартов могут относиться современные документы RFC:

– к стандартам отдельных фирм;

– к государственным стандартам;

– к национальным стандартам;

– к международным стандартам.

16. Какая организация стояла у истоков создания и стандартизации стека TCP/IP?

17. Определите основные особенности стека TCP/IP.

18. Сравните функции самых нижних уровней моделей TCP/IP и OSI.

19. Дайте определение транспортных и информационных услуг.

20. Какие протоколы относятся к слою управления (control plane)? А к слою менеджмента

(management plane)?

21. Должны ли маршрутизаторами поддерживаться протоколы транспортного уровня?

22. Пусть на двух компьютерах установлено идентичное программное и аппаратное обеспечение за исключением того, что драйверы сетевых адаптеров Ethernet поддерживают отличающиеся интерфейсы с протоколом сетевого уровня IP. Будут ли эти компьютеры нормально взаимодействовать, если их соединить в сеть?

23. Как организовать взаимодействие двух компьютеров, если у них отличаются протоколы:

– физического и канального уровней;

– сетевого уровня;

– прикладного уровня.

24. Опишите ваши действия в случае, если вам необходимо проверить, на каком этапе находится процесс стандартизации технологии MPLS?

14.1.4. Темы контрольных работ

Виды беспроводных сетей.

Угрозы информационной безопасности в системах беспроводной связи.

Построение защищенных распределенных систем на основе беспроводных сетей.

14.1.5. Темы лабораторных работ

Методы защиты от подслушивания в системах беспроводной связи.

Угроза типа "Отказ в обслуживании". Способы защиты.

Устройства глушения беспроводной связи.

Криптозащита в системах беспроводной связи.

Построение распределенной системы беспроводной связи.

Проведение оценки защищенности системы беспроводной связи.

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

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

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

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

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

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

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

– методом чтения ассистентом задания вслух;
– предоставление задания с использованием сурдоперевода.

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

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

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

Для лиц с нарушениями зрения:

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

Для лиц с нарушениями слуха:

– в форме электронного документа;
– в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

– в форме электронного документа;
– в печатной форме.

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