

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Беспалов Владимир Александрович

Должность: Ректор МИЭТ

Дата подписания: 01.09.2023 14:12:11

Уникальный программный ключ:

ef5a4fe6ed0ffdf3f1a49d6ad1b49464dc1bf7354f736d76c8f8de4882b8d602

МИНОБРНАУКИ РОССИИ

Федеральное государственное автономное образовательное учреждение высшего образования

«Национальный исследовательский университет

«Московский институт электронной техники»



УТВЕРЖДАЮ

Проректор по учебной работе

И.Г.Игнатова

«23» *марта* 2021 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

«Безопасность телекоммуникационных систем»

Направление подготовки – 10.03.01 «Информационная безопасность»

Направленность (профиль) – «Техническая защита информации»

2021 г.

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ

Дисциплина участвует в формировании следующих подкомпетенций:

Компетенции	Подкомпетенции, формируемые в дисциплине	Индикаторы достижения подкомпетенций
ОПК-9. Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ОПК-9.БТКС. Способен применять средства защиты информации для обеспечения безопасности телекоммуникационных систем	Знания: беспроводных технологии локальной передачи данных; общих характеристик стандартов сотовой связи и беспроводного доступа; общие характеристики и возможности систем и средств радиоразведки; возможные виды атак на беспроводные сети; основы безопасности беспроводных технологий; основы обеспечения безопасности беспроводных сетей сотовой связи; основы основные направления и методы обеспечения помехозащищенности РЭС и обеспечения ЭМС РЭС; Умения: проводить анализ угроз безопасности беспроводных сетей связи; проводить выбор методов и средств по защите информации в беспроводных сетях связи; разрабатывать политику безопасности корпоративной беспроводной сети; проводить настройку безопасности корпоративной беспроводной сети; проводить оценку безопасности информации, передаваемой в беспроводной сети связи. Опыт деятельности: анализа угроз безопасности беспроводных сетей связи; обоснования методов и средств по защите информации в беспроводных сетях связи.

В результате изучения дисциплины студент должен:

Знать:

- беспроводные технологии локальной передачи данных;
- общие характеристики стандарта GSM, состав оборудования, сетевые и радиоинтерфейсы; принципы построения системы сетевого управления и распределение функций сетевого управления в GSM, стандартные интерфейсы в системе сетевого управления GSM
- общие характеристики стандарта телефонной радиосвязи DECT;
- общие характеристики беспроводная мобильная связь WiMAX;
- общие характеристики стандарта связи CDMA (IS-95);
- общие характеристики и возможности систем и средств радиоразведки;
- общие характеристики и возможности средств портативных средства радиоразведки;
- возможные виды атак на беспроводные сети;
- основы безопасности беспроводных технологий;
- основы обеспечения безопасности беспроводных сетей сотовой связи;
- особенности обеспечения безопасности в стандартах 802.11 и 802.16;
- особенности обеспечения безопасности в стандарте DECT;
- особенности обеспечения безопасности CDMA сетей;
- классификацию радиопомех. Преднамеренные радиопомехи. Непреднамеренные радиопомехи;
- средства радиоподавления беспроводных сетей связи;
- основные направления и методы обеспечения помехозащищенности РЭС;
- основы обеспечения электромагнитной совместимости РЭС.

Уметь:

- проводить анализ угроз безопасности беспроводных сетей связи;
- проводить обоснованный выбор методов и средств по защите информации в беспроводных сетях связи;
- разрабатывать политику безопасности корпоративной беспроводной сети;
- проводить настройку безопасности корпоративной беспроводной сети;
- проводить оценку безопасности информации, передаваемой в беспроводной сети связи;
- проводить расчет зон радиоподавления средств сотовой связи и беспроводного доступа.

Иметь опыт деятельности:

- проведения анализа угроз безопасности беспроводных сетей связи;
- обоснования методов и средств по защите информации в беспроводных сетях связи.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Безопасность телекоммуникационных систем» входит в обязательную часть Блок 1 «Дисциплины (модули)» образовательной программы. Дисциплина читается на 4-м курсе в 7-м семестре.

Изучение дисциплины «Безопасность телекоммуникационных систем» базируется на дисциплинах образовательной подготовки (ОП) бакалавриата по направлению подготовки

10.03.01 «Информационная безопасность» и профилю подготовки «Техническая защита информации»: «Информационные технологии 1. Операционные системы», «Информационные технологии 2. Базы данных», «Информационные технологии 3. Вычислительные сети», «Защита информации от несанкционированного доступа»

Знания и практические навыки, полученные в результате изучения дисциплины, используются в производственной практике и при подготовке выпускной квалификационной работы.

3. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Курс	Семестр	Общая трудоёмкость (ЗЕ)	Общая трудоёмкость (часы)	Контактная работа, часы					Самостоятельная работа, часы	Вид промежуточной аттестации
				ВСЕГО	Лекции	Лабораторные работы	Практические занятия	Групповые консультации		
4	7	4	144	80	32	-	32	16	64	ЗаО

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Номер и наименование модуля	Контактная работа, часы				Самостоятельная работа, часы	Формы текущего контроля
	Лекции	Лабораторные работы	Практические занятия	Групповые консультации		
1. Основные архитектурно-технические решения беспроводных систем связи различных уровней	8	-	4	4	12	Компьютерный тест (РК 1)
2. Способы и средства перехвата информации, передаваемой в беспроводных системах и сетях связи	4	-	4	2	8	Компьютерный тест (РК 2) Зачет по ПЗ № 3

Номер и наименование модуля	Контактная работа, часы				Самостоятельная работа, часы	Формы текущего контроля
	Лекции	Лабораторные работы	Практические занятия	Групповые консультации		
3. Методы и средства обеспечения безопасности информации в беспроводных системах связи	12	-	20	8	32	Компьютерный тест (РК 3) Зачет по ПЗ № 4 – 7
4. Радиоэлектронная защита беспроводных систем связи	8	-	4	2	12	Компьютерный тест (РК 4) Зачет по ПЗ № 8

4.1. Лекционные занятия

№ модуля дисциплины	№ лекции	Объем занятий (часы)	Краткое содержание
1	1.	2	Беспроводные технологии локальной передачи данных. Беспроводная связь по технологии Bluetooth, классы оборудования, частотный диапазон, модуляция GFSK, псевдослучайное переключение частот, протоколы, профили узлов, установление связи, поддержание обмена, стандарты 802.15, релизы Bluetooth, проблема совместимости. Локальные беспроводные сети стандарта 802.11., канальный и физический уровень OSI, организация WLAN (режим инфраструктуры и режим «точка-точка»), расширение LAN («мосты»), организация доступа в Интернет, технологии передачи данных DSSS и OFDM, ячеистые сети (802.11.s), стандарты WiFi, проблемы совместимости.
	2.	2	Цифровая сотовая система мобильной радиосвязи стандарта GSM. Общие характеристики стандарта GSM, структурная схема и состав оборудования, сетевые и радиоинтерфейсы. Структура служб и передача данных в стандарте GSM, структура TDMA кадров и формирование сигналов в стандарте GSM. Организация физических и логических каналов в стандарте GSM, частотный план стандарта GSM, структура логических кана-

№ модуля дисциплины	№ лекции	Объем занятий (часы)	Краткое содержание
			лов связи, структура логических каналов управления, организация физических каналов, модуляция радиосигнала. Кодирование и перемежение в полноскоростном канале передачи данных и в каналах управления. Общее описание процессов обработки речи для стандарта GSM. Принципы построения системы сетевого управления и распределение функций сетевого управления в GSM, стандартные интерфейсы в системе сетевого управления GSM
	3.	2	Стандарт телефонной радиосвязи DECT. Частотный диапазон, модуляция GMSK, функции каналов, структура пакетов, организация пакетов в кадры, технологии множественного доступа с временным (TDMA) и частотным (FDMA) разделением, дуплексный канал с временным разделением (TDD). Расширение DECT/GAP для обеспечения совместимости производителей оборудования, использование в IP-телефонии. Высокоскоростная беспроводная мобильная связь WiMAX, архитектура и принцип работы, частотные диапазоны, развитие технологии OFDM для абонентов (OFDMA), принцип разделения приоритета доступа, режимы работы (фиксированный, сессионный, портативный, мобильный вариант), широкополостный доступ, MAC – уровень обработки сигнала и канальный уровень обработки данных, стандарты 802.16..
	4.	2	Беспроводные сети мобильной связи. Стандарт связи CDMA (IS-95), расширение спектра и разделение каналов по технологии кодовой модуляции и множественного доступа, частотный диапазон, методы модуляции несущей частоты QPSK(BTS) и O-QPSK(MS), прямые и обратные каналы связи, состав каналов, порядок прохождения речевого сигнала в мобильном терминале до отправки в эфир. Беспроводные глобальные сети GPRS, EDGE, EV-DO.
2	5.	2	Системы и средства радиоразведки. Системы и средства космической радио-, радиотехнической разведки. Системы и средства воздушной радио-, радиотехнической разведки. Системы и средства наземной радиоразведки.
	6.	2	Портативные средства радиоразведки. Портативные радиопеленгаторы. Портативные средства радиоразведки. Средства перехвата сотовой связи. Средства перехвата сетей беспроводного доступа
3	7.	2	Безопасность беспроводных технологий. Цели и задачи защиты данных в беспроводных сетях. Возможные виды атак на беспроводные сети, атаки на сетевой трафик, угрозы подмены аба-

№ модуля дисциплины	№ лекции	Объем занятий (часы)	Краткое содержание
			нента и сотовой станции, клонирование и хищение оборудования, атаки для получения бесплатного доступа к услугам сети (хищение трафика), получение идентификатора сети SSID, модель нарушителя. Предотвращение угроз безопасности беспроводных сетей, архитектура и протоколы защиты, обеспечение идентичности пользователя в мобильных и локальных беспроводных сетях, безопасность беспроводного широкополосного доступа, защита данных от ошибок в беспроводных сетях
	8.	2	Безопасность беспроводных сетей сотовой связи. Стандарт криптографических технологий в системах сотовой связи TIA95, криптографические примитивы, функция перемешивания для аутентификации и генерации ключей, повторяющаяся XOR-маска для наложения на голосовые данные, потоковый шифр для беспроводного доступа к данным, блочный шифр для шифрования служебных сообщений. Система функций Уолша, применение для закрытия дискретного сигнала.
	9.	2	Безопасность в стандарте 802.11. Протокол аутентификации с совместно используемым ключом (WEP), проверка целостности пакетов (CRC-32), протокол безопасности WPA/WPA2, временный протокол целостности ключа TKIP, протокол расширенной аутентификации EAP, беспроводные виртуальные частные сети, технология скрытия идентификатора сети ESSID, фильтрация MAC-адресов
	10.	2	Безопасность в стандарте 802.16. Защищенные связи для данных и для авторизации, расширяемый протокол аутентификации, протокол авторизации и ключей шифрования, обмен ключами, шифрование данных, использование DES и AES, блок сцепления шифров, блок шифрования счетчика, создание и шифрование кодов аутентификации сообщений, шифрование информационной части сообщений. Безопасность в стандарте радиотелефонии DECT, шифрование DECT Standard Cipher (DSC), вектор инициализации.
	11.	2	Безопасность в стандарте GSM. Общее описание характеристик безопасности, механизмы аутентификации, секретность передачи данных, криптографические алгоритмы A3, A8, и A5(A5/1 и A5/2), управление ключами, обеспечение секретности абонента, обеспечение секретности в процедуре корректировки местоположения, общий состав секретной информации и ее распределение в аппаратных средствах GSM, обеспечение секретности при обмене сообщениями между HLR, VLR и MSC, модуль подлинности абонента.
	12.	2	Безопасность CDMA сетей.

№ модуля дисциплины	№ лекции	Объем занятий (часы)	Краткое содержание
			Управление ключами, генерация аутентификационного ключа, использование серийного номера устройства и случайных факторов для генерации секретных данных SSD, структура SSD, счетчики вызовов и OTASP-процедура согласования ключей для защиты от подмены абонента («двойники»), Генерация и использование частной и модифицированной кодовой маски для закрытия голосового сообщения, алгоритм шифрования служебных сообщений CMEA, генерация и использование Data-key и ORYX-процедуры для шифрования потока информации по каналу связи.
4	13.	2	Преднамеренные и непреднамеренные радиопомехи. Классификация радиопомех. Преднамеренные радиопомехи. Непреднамеренные радиопомехи.
	14.	2	Средства радиоподавления беспроводных сетей связи. Системы и комплексы радиоэлектронной борьбы. Блокираторы средств сотовой связи. Блокираторы средств беспроводного доступа
	15.	2	Защита радиоэлектронных средств от преднамеренных радиопомех Основные направления обеспечения помехозащищенности РЭС. Показатели помехозащищенности РЭС. Показатели скрытности РЭС. Методы обеспечения скрытности РЭС. Показатели помехоустойчивости РЭС. Методы обеспечения помехоустойчивости РЭС.
	16.	2	Обеспечение электромагнитной совместимости РЭС Параметры РЭС, влияющие на ЭМС. Восприимчивость радиоприемных устройств к радиопомехам. Методы обеспечения ЭМС РЭС

4.2. Практические занятия

№ модуля дисциплины	№ практического занятия	Объем занятий (часы)	Краткое содержание
1	1.	4	Практическое занятие (семинар). Системы и средства сотовой связи и беспроводного доступа Цифровая сотовая система мобильной радиосвязи стандарта GSM. Стандарт телефонной радиосвязи DECT. Высокоскоростная беспроводная мобильная связь WiMAX Стандарт связи CDMA
2	2.	4	Практическое занятие (семинар). Портативные системы и средства

			радиоразведки Портативные радиопеленгаторы. Портативные средства радиоразведки. Средства перехвата сотовой связи. Средства перехвата сетей беспроводного доступа
3	3.	4	Практическое занятие (групповое упражнение). Оценка возможностей средств радиоразведки по перехвату информации, передаваемой по каналам радиосвязи. Расчет дальности радиоразведки мобильных РЭС. Расчет ошибки определения координат мобильных РЭС.
	4.	4	Практическое занятие (групповое упражнение). Модули идентификации абонента мобильной связи. Карты SIM, USIM, R-USIM, структура служб, функции и предоставляемые услуги по безопасности.
	5.	4	Практическое занятие (групповое упражнение). Анализ методов, технологий и возможностей «взлома» архитектуры беспроводной корпоративной сети. Анализ методов, технологий и возможностей «взлома» протоколов аутентификации и шифрования
	6.	4	Практическое занятие (групповое упражнение). Настройка безопасности корпоративной беспроводной сети. Решения по безопасности в системах беспроводной связи третьего поколения. Безопасное взаимодействие беспроводных сетей с внешним сетевым оборудованием, защита данных в коммутационной инфраструктуре систем мобильной связи.
	7.	4	Практическое занятие (групповое упражнение). Разработка политики безопасности корпоративной беспроводной сети
4	8.	4	Практическое занятие (групповое упражнение). Расчет зон радиоподавления средств сотовой связи и беспроводного доступа.

4.3. Лабораторные работы

Не предусмотрены

4.4. Самостоятельная работа студентов

№ модуля дисциплины	Объем занятий (часы)	Вид СРС
1	4	Подготовка к практическому занятию (семинару) № 1: Изучение материалов лекции №№ 1- 4 и рекомендованной литературы. Изучение плана проведения семинара № 1. Подготовка доклада и презентации по одному из вопросов семинара
2	4	Подготовка к практическому занятию (семинару) № 2: Изучение материалов лекции №№ 5 - 6 и рекомендованной литературы.

№ модуля дисциплины	Объем занятий (часы)	Вид СРС
		Изучение плана проведения семинара № 2. Подготовка доклада и презентации по одному из вопросов семинара
3	4	Подготовка к практическому занятию (групповому упражнению) № 3: Изучение материалов лекции №№ 7 - 12 и рекомендованной литературы. Изучение методических рекомендаций по проведению практического занятия № 3
	4	Подготовка к практическому занятию (групповому упражнению) № 4: Изучение материалов лекции №№ 7 - 12 и рекомендованной литературы. Изучение методических рекомендаций по проведению практического занятия № 4
	4	Подготовка к практическому занятию (групповому упражнению) № 5: Изучение материалов лекции №№ 7 - 12 и рекомендованной литературы. Изучение методических рекомендаций по проведению практического занятия № 5
	4	Подготовка к практическому занятию (групповому упражнению) № 6: Изучение материалов лекции №№ 7 - 12 и рекомендованной литературы. Изучение методических рекомендаций по проведению практического занятия № 6
	4	Подготовка к практическому занятию (групповому упражнению) № 7: Изучение материалов лекции №№ 7 - 12 и рекомендованной литературы. Изучение методических рекомендаций по проведению практического занятия № 7
4	4	Подготовка к практическому занятию (групповому упражнению) № 8: Изучение материалов лекции №№ 13 - 16 и рекомендованной литературы. Изучение методических рекомендаций по проведению практического занятия № 8
1	4	Подготовка к компьютерному тесту КТ 1. Изучение материалов лекции №№ 1 - 4 и рекомендованной литературы.
2	4	Подготовка к компьютерному тесту КТ 2. Изучение материалов лекции №№ 5 - 6 и рекомендованной литературы.
3	4	Подготовка к компьютерному тесту КТ 3. Изучение материалов лекции №№ 7 - 12 и рекомендованной литературы.
4	4	Подготовка к компьютерному тесту КТ 4. Изучение материалов лекции №№ 13 - 16 и рекомендованной литературы.
1- 4	16	Подготовка к сдаче зачета

4.5. Примерная тематика курсовых работ (проектов)

Не предусмотрены

5. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Учебно-методическое обеспечение для самостоятельной работы студентов в составе УМК дисциплины (ОРИОКС, <http://orioks.miet.ru/>):

Модуль 1. Основные архитектурно-технические решения беспроводных систем связи различных уровней

Информационно-справочный материал к практическому занятию № 1. ОРИОКС// URL: <http://orioks.miet.ru/>

Методические рекомендации студентам по подготовке и проведению практического занятия № 1. ОРИОКС// URL: <http://orioks.miet.ru/>

Модуль 2. Способы и средства перехвата информации, передаваемой в беспроводных системах и сетях связи

Информационно-справочный материал к практическому занятию № 2. ОРИОКС// URL: <http://orioks.miet.ru/>

Методические рекомендации студентам по подготовке и проведению практического занятия № 2. ОРИОКС// URL: <http://orioks.miet.ru/>

Модуль 3. Методы и средства обеспечения безопасности информации в беспроводных системах связи

Информационно-справочный материал к практическим занятиям № 4 – 7. ОРИОКС// URL: <http://orioks.miet.ru/>

Методические рекомендации студентам по подготовке и проведению практических занятий № 4 – 7.. ОРИОКС// URL: <http://orioks.miet.ru/>

Модуль 4. Радиоэлектронная защита беспроводных систем связи

Информационно-справочный материал к практическому занятию № 8. ОРИОКС// URL: <http://orioks.miet.ru/>

Методические рекомендации студентам по подготовке и проведению практического занятия № 8. ОРИОКС// URL: <http://orioks.miet.ru/>

6. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ

Литература

1. Берлин А.Н. Сотовые системы связи / А.Н. Берлин. - 2-е изд. - М. : ИНТУИТ, 2016. - 430 с. - URL: <https://e.lanbook.com/book/100494> (дата обращения: 15.03.2021). - ISBN 978-5-9963-0104-1 .
2. Берлин А.Н. Телекоммуникационные сети и устройства / А.Н. Берлин. - 2-е изд. - М. : ИНТУИТ, 2016. - 395 с. - URL: <https://e.lanbook.com/book/100525> (дата обращения:

15.03.2021). - ISBN 978-5-94774-896-3 .

3. Программно-аппаратные средства защиты информации : учебное пособие / В. А. Воеводин, А. В. Душкин, А. Н. Петухов, А. А. Хорев; Министерство образования и науки РФ, Национальный исследовательский университет "МИЭТ"; под редакцией А.А. Хорева. - Москва : МИЭТ, 2021. - 280 с. - ISBN 978-5-7256-0972-1.
4. Программно-аппаратные средства защиты информации : учебно-методическое пособие / А. В. Душкин, О. Р. Лукманова, А. Н. Петухов, А. А. Хорев; Министерство образования и науки РФ, Национальный исследовательский университет "МИЭТ"; под редакцией А.А. Хорева. - Москва : МИЭТ, 2021. - 216 с. - ISBN 978-5-7256-0958-5 .
5. Управление безопасностью критических информационных инфраструктур : учебное пособие / А. Н. Петухов, П. Л. Пилюгин, А. В. Душкин, Ю. А. Губсков; Министерство образования и науки РФ, Национальный исследовательский университет "МИЭТ"; под редакцией А.В. Душкина. - Москва : МИЭТ, 2021. - 208 с. - ISBN 978-5-7256-0973-8
6. Хорев А.А. Техническая защита информации : Учеб. пособие: В 3-х т. Т. 1 : Технические каналы утечки информации / А.А. Хорев; М-во образования и науки РФ, Федеральное агентство по образованию, МИЭТ(ТУ). - М. : НПЦ Аналитика, 2008. - 436 с. - ISBN 978-59901488-1-9 .

Периодические издания

1. Защита информации. Inside : информационно-методический журнал / Издательский дом "Афина". - Санкт-Петербург : ИД Афина, 2004 - . - URL: <http://elibrary.ru/contents.asp?titleid=25917> (дата обращения: 15.03.2021). - Режим доступа: по подписке (2017-2021). - ISSN 2413-3582.
2. Безопасность информационных технологий : научный журнал / ФГАОУ ВО "Национальный исследовательский ядерный университет "МИФИ". - Москва : НИЯУ МИФИ, 1994 - . - URL: <https://bit.mephi.ru/index.php/bit/index> (дата обращения: 16.03.2021). - Режим доступа: свободный. - ISSN 2074-7128 (Print); 2074-7136 (Online).
3. Вестник УрФО. Безопасность в информационной сфере: научный журнал/ Южно-Уральский государственный университет (национальный исследовательский университет). - Челябинск: УрГУ, 2011 - 2018. - URL: <http://info-secur.ru/index.php/ojs/issue/archive> (дата обращения: 16.03.2021). - Режим доступа: свободный. - ISSN 2225-5435 (Print).
4. Информация и безопасность: научный журнал / ФГБОУ ВО "Воронежский государственный технический университет" (ВГТУ). - Воронеж : ВГТУ, 1998 - . - URL: https://www.elibrary.ru/title_about_new.asp?id=8748 (дата обращения: 15.03.2021). - Режим доступа: для зарегистрированных пользователей. - ISSN 1682-7813.

7. ПЕРЕЧЕНЬ ПРОФЕССИОНАЛЬНЫХ БАЗ ДАННЫХ, ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ

1. eLIBRARY.RU: Научная электронная библиотека: сайт. - Москва, 2000 -. - URL: <https://www.elibrary.ru> (дата обращения: 16.03.2021). – Текст: электронный.
2. ЛАНЬ: электронно-библиотечная система: сайт. – Санкт-Петербург, 2010 -. - URL: <https://e.lanbook.com> (дата обращения: 10.03.2021). - Текст: электронный.
3. ФСТЭК России: Государственный реестр сертифицированных средств защиты информации. – Москва, 2014. - . - URL: <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii> (дата обращения: 10.03.2021). - Текст: электронный.

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В ходе реализации обучения используется смешанное обучение, которое основано на интеграции технологий традиционного и электронного обучения, замещении части традиционных учебных форм занятий формами и видами взаимодействия в электронной образовательной среде.

Освоение образовательной программы обеспечивается ресурсами электронной информационно-образовательной среды ОРИОКС <http://orioks.miet.ru>.

Для взаимодействия студентов с преподавателем используются сервисы обратной связи: ОРИОКС «Домашние задания», электронная почта преподавателя.

В процессе обучения при проведении занятий и для самостоятельной работы используются внутренние электронные ресурсы (<http://orioks.miet.ru>).

Тестирование проводится в ОРИОКС (MOODLe).

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Наименование учебных аудиторий и помещений для самостоятельной работы	Оснащенность учебных аудиторий и помещений для самостоятельной работы	Перечень программного обеспечения
Учебная аудитория	Мультимедийное оборудование: компьютер с программным обеспечением, возможностью подключения к сети Интернет и обеспечением доступа в электронно-образовательную среду	Операционная система Microsoft Windows от 7 версии и выше; Microsoft Office или Open Office, браузер (Firefox/Google Chrome/Explorer).

Наименование учебных аудиторий и помещений для самостоятельной работы	Оснащенность учебных аудиторий и помещений для самостоятельной работы	Перечень программного обеспечения
	МИЭТ; телевизор/проектор; акустическое оборудование (микрофон, звуковые колонки), вебкамера с микрофоном). Учебная доска.	
Учебная аудитория № 3226: Лаборатория «Технологий и управления информационной безопасностью»	1. Автоматизированное рабочее место преподавателя (АРМ-П): ПЭВМ Flagman-G в составе: Монитор 22" Samsung S22B370H, HDMI (LED); ИБП APC BK650EI; Клавиатура Logitech K120 USB; Манипулятор Logitech B110 – 1 шт. 2. Автоматизированное рабочее место студента (АРМ-С): ПЭВМ Flagman-G в составе: корпус InWin S617 450W; Источник бесперебойного питания APC BK650EI; Клавиатура Logitech K120 USB; Манипулятор Logitech B110 – 27 шт.	1. Операционная система Microsoft Win Pro 7 2. Неисключительное право на использование Microsoft Office Std 2013 RUS OLP NL (Из реестра МИЭТ п.18) – 28 шт. 3. Лиц. на ПО Multisim 9 Academic Edituon Single seal (Из реестра МИЭТ п.78) – 28 шт. 4. Корпоративная информационно - технологическая платформа ОРИОКС (Из реестра МИЭТ п.88) – 28 шт.
Помещение для самостоятельной работы обучающихся: Учебная аудитория № 3226	Компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в ОРИОКС: 1. Автоматизированное рабочее место преподавателя (АРМ-П): ПЭВМ Flagman-G в составе:	1. Неисключительное право на использование операционной системы Microsoft Win Pro 7 2. Неисключительное право на использование Microsoft Office Std 2013 RUS OLP NL 3. Лиц. на ПО Multisim 9 Academic Edituon Single seal 4. Корпоративная информацион-

Наименование учебных аудиторий и помещений для самостоятельной работы	Оснащенность учебных аудиторий и помещений для самостоятельной работы	Перечень программного обеспечения
	ве: Монитор 22" Samsung S22B370H, HDMI (LED); ИБП APC BK650EI; Клавиатура Logitech K120 USB; Манипулятор Logitech B110 – 1 шт. 2. Автоматизированное рабочее место студента (АРМ-С): ПЭВМ Flagman-G в составе: корпус InWin S617 450W; Источник бесперебойного питания APC BK650EI; Клавиатура Logitech K120 USB; Манипулятор Logitech B110 – 27 шт.	но - технологическая платформа ОРИОКС

10. ФОНДЫ ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕРКИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ/ПОДКОМПЕТЕНЦИЙ

ФОС по подкомпетенции ОПК-9. БТКС. Способен применять средства защиты информации для обеспечения безопасности телекоммуникационных систем.

Фонды оценочных средств представлены отдельными документами и размещены в составе УМК дисциплины электронной информационной образовательной среды ОРИОКС// URL: <http://orioks.miet.ru/>.

11. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

В целях практической подготовки в дисциплине предусмотрены практические занятия (семинары и групповые упражнения).

Каждое практическое занятие направлено на формирование отдельных умений, необходимых для формирования общепрофессиональных и профессиональных компетенции.

11.1. Методические указания студентам по подготовке к семинарам

Семинар - развернутая беседа с обсуждением доклада. Проводится на основе заранее разработанного плана, по вопросам которого готовится вся учебная группа. Основными компонентами такого занятия являются: вступительное слово преподавателя, доклады обучающихся, вопросы докладчикам, выступления студентов по докладу и обсуждаемым вопросам, заключение преподавателя.

Развернутая беседа позволяет вовлечь в обсуждение проблем наибольшее число обучающихся. Главная задача преподавателя при проведении такого семинарского занятия состоит в использовании всех средств активизации: постановки хорошо продуманных, четко сформулированных дополнительных вопросов, умелой концентрации внимания на наиболее важных проблемах, умения обобщать и систематизировать высказываемые в выступлениях идеи, сопоставлять различные точки зрения, создавать обстановку свободного обмена мнениями. Данная форма семинара способствует выработке у обучающихся коммуникативных навыков.

Как правило, темы докладов разрабатываются преподавателем заранее и включаются в планы семинаров. Доклад носит характер краткого (10-15 мин.) аргументированного изложения одной из центральных проблем семинарского занятия с использованием презентации.

11.2. Методические указания студентам по подготовке к групповым упражнениям

Ведущей дидактической целью групповых упражнений является формирование практических умений выполнять определенные действия, операции, необходимые в последующем в профессиональной деятельности.

Групповые упражнения носят репродуктивный характер и отличаются тем, что при их проведении студенты пользуются подробными инструкциями, в которых указаны: цель работы, пояснения (теория), порядок выполнения работы, таблицы, выводы (без формулировки), контрольные вопросы, учебная и специальная литература.

Формы организации студентов на групповых упражнениях: индивидуальная, при которой каждый студент выполняет индивидуальное задание.

Для проведения групповому упражнению преподавателями разрабатываются методические рекомендации по их выполнению, которые рассматриваются и утверждаются на заседании кафедры. Методические рекомендации разрабатываются по каждому групповому упражнению, предусмотренными рабочей программой учебной дисциплины: в соответствии с количеством часов, требованиями к знаниям и умениям, темой практических занятий, установленными рабочей программой учебной дисциплины по соответствующим разделам (темам).

Методические рекомендации по выполнению группового упражнения (ГУ) включают в себя:

- пояснительную записку;
- наименование раздела (темы);
- объем учебного времени, отведенный на ГУ;
- наименование темы ГУ;
- цель ГУ (в т.ч. требования к знаниям и умениям студентов, которые должны быть реализованы);
- перечень необходимых средств обучения (оборудование, материалы и др.);

- требования по теоретической готовности студентов к выполнению ГУ (требования к знаниям, перечень дидактических единиц);
- содержание заданий;
- рекомендации (инструкции) по выполнению заданий;
- требования к результатам работы, в т.ч. к оформлению;
- критерии оценки и формы контроля;
- список рекомендуемой литературы;
- приложения.

При подготовке к ГУ студенту необходимо:

- уяснить вопросы и задания, рекомендуемые для подготовки к ГУ;
- ознакомиться с методическими рекомендациями по выполнению ГУ;
- прочитать конспект лекций и соответствующие главы учебника (учебного пособия), дополнить запись лекций выписками из него;
- прочитать дополнительную литературу, рекомендованную преподавателем. Наиболее интересные мысли следует выписать;
- сформулировать и записать развернутые ответы на вопросы для подготовки к ГУ;
- подготовить отчеты для заполнения.

На ГУ студент должен выполнить задание в соответствии с методическими указаниями.

Отчет по ГУ должен быть оформлен в соответствии с методическими указаниями и ГОСТами.

При защите отчета по ГУ убедительно четко и аргументировано изложить содержание проведенных исследований и выводы по полученным результатам.

По завершению занятия студент должен уяснить недостатки, указанные преподавателем при необходимости записать их содержание.

Студенты, по каким-либо причинам, отсутствовавшие на занятии, в свободное время должны самостоятельно изучить учебный материал и выполнить ГУ, после чего отчитаться в проделанной работе перед преподавателем.

Студенты на ГУ обязаны соблюдать меры безопасности при работе на аппаратуре (оборудовании). Перед началом занятий, каждый студент должен пройти инструктаж по соблюдению мер безопасности на рабочем месте и уяснить места расположения средств пожаротушения и обесточивания аппаратуры (оборудования).

Каждое практическое занятие – групповое упражнение направлено на формирование отдельных умений, необходимых для формирования компетенций и подкомпетенций.

11.3. Система контроля и оценивания

Для оценки успеваемости студентов по дисциплине используется накопительно-балльная система.

Под накопительно-балльной системой понимается система количественной, балльно-рейтинговой оценки качества освоения учебной дисциплины студентом $R_{\text{нак}}$ по суммарному результату текущего $R_{\text{тек}}$ и итогового контроля $R_{\text{итог}}$, с учетом посещаемости студентом занятий, его активности на занятиях и качества выполнения им текущих заданий $R_{\text{пр}}$.

Выполнение контрольных мероприятий текущего контроля (сдача компьютерных тестов, защита отчетов по практическим занятиям), посещаемость занятий и активность на занятиях, результаты итогового контроля (сдача зачета) оцениваются баллами, общая сумма

которых составляет 100 баллов (максимальное значение нормативного рейтинга учебной дисциплины – $R_{нор}$).

Структура и график контрольных мероприятий приведены в таблице 11.1.

Таблица 11.1

Структура и график контрольных мероприятий

Неделя	Название контрольного мероприятия	Баллы	
		максимальный балл	минимальный положительный
5	Практическое занятие (семинар) № 1	8	4
5	Компьютерный тест КТ-1	4	2
7	Практическое занятие (семинар) № 2	8	4
7	Компьютерный тест КТ-2	4	2
11	Практическое занятие (групповое упражнение) № 3.	8	4
12	Практическое занятие (групповое упражнение) № 4.	8	4
13	Практическое занятие (групповое упражнение) № 5	8	4
	Компьютерный тест КТ-3	4	2
16	Практическое занятие (групповое упражнение) № 6.	8	4
16	Компьютерный тест КТ-4	4	2
16	Активность, посещаемость	6	3
	Итого за текущий контроль	70	35
18	Итоговый контроль	30	15
	Накопленный рейтинг	100	50

В зачетную ведомость и зачетную книжку вносится не зачетная оценка по дисциплине, а **итоговая 5-балльная оценка** за семестр, рассчитанная на основе накопленных рейтинговых баллов по результатам семестрового и итогового контроля учебной дисциплины.

Итоговая оценка студенту по дисциплине за семестр по 5-ти балльной шкале выставляется на основе накопленной им общей суммы баллов $R_{нак}$ по итогам семестрового и итогового контроля. При выставлении итоговой оценки используется шкала, приведенная в таблице:

Сумма баллов	Оценка
Менее 50	2
50 – 69	3
70 – 85	4
86 – 100	5

Положительная оценка («отлично», «хорошо», «удовлетворительно») заносится в зачетную ведомость и зачетную книжку студента. Оценка «неудовлетворительно» проставляется только в зачетную ведомость.

РАЗРАБОТЧИК

Доцент кафедры «Информационная безопасность»

кандидат технических наук, профессор _____



А.Н.Петухов

Рабочая программа дисциплины «Безопасность телекоммуникационных систем» по направлению подготовки 10.03.01 «Информационная безопасность», направленности (профилю) «Техническая защита информации» разработана на кафедре «Информационная безопасность» и утверждена на заседании кафедры 17 марта 2021 года, протокол № 3.

Заведующий кафедрой «Информационная безопасность»

доктор технических наук, профессор _____

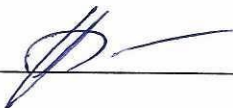


А.А.Хорев

Лист согласования

Рабочая программа согласована с Центром подготовки к аккредитации и независимой оценки качества

Начальник АНОК _____



/ И.М.Никулина /

Рабочая программа согласована с библиотекой МИЭТ

/ Директор библиотеки _____



/ Т.П.Филиппова /