Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«Национальный исследовательский университет
«Московский институт электронной техники»

УТВЕРЖДАЮ
Проректор по учебной работе
_____ И.Г. Игнатова
«25» 12 2020 г.
М.П.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

«Безопасность телекоммуникационных систем»

Направление подготовки - 11.03.02 «Инфокоммуникационные технологии и системы связи»

Направленность (профиль) – «Сети и системы инфокоммуникаций»

Москва 2020

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ

Дисциплина участвует в формировании следующих компетенцийобразовательных программ:

Компетенция ПК-7 «Способен к администрированию средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов)**» сформулирована на основе профессионального стандарта 06.027**«Специалист по администрированию сетевых устройств информационно-коммуникационных систем».

Обобщенная трудовая функция D Администрирование процесса управления безопасностью сетевых устройств и программного обеспечения.

Трудовая функция D/03.6 Администрирование средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов).

Подкомпетенции, формируемые в дисциплине	**Задачи профессиональной деятельности**	**Индикаторы достижения подкомпетенций**
ПК-7.БТС Администрирование средств обеспечения безопасности телекоммуникационных систем	Параметризация настроек средств защиты информации телекоммуникационных систем и систем связи; Установка дополнительных программных и аппаратно-программных продуктов для обеспечения безопасности удаленного доступа и их параметризация; Настройка средств обеспечения безопасности удаленного доступа и специализированных защищенных протоколов; Документирование настроек средств обеспечения безопасности.	Знания: Общих принципов функционирования аппаратных, программных и программно-аппаратных средств защиты информации; Архитектуры аппаратных, программных и программно-аппаратных средств защиты информации; Принципов функционирования защищенных протоколов канального, сетевого, транспортного и прикладного уровней; Принципов обеспечения безопасности в моделивзаимодействия открытых систем; Основ криптографической защиты информации; Умения: Подключать и настраивать современные средства защиты информации; Пользоваться нормативно-технической документацией в области безопасности

		инфокоммуникационных технологий; Работать с контрольно-измерительными аппаратными и программными средствами. Опыт деятельности: Использование и настройка средств виртуализации вычислительной среды; Использование средств анализа сетевого трафика; Использовать средства криптографической защиты информации (шифрования и цифровой подписи); Использовать средства каталогизации доступа к информационным ресурсам; Анализа рисков и формирования требований безопасности к телекоммуникационным системам и устройствам; Использовать средства построения виртуальных частных сетей.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина входит в часть, формируемую участниками образовательных отношений Блока 1 «Дисциплины (модули)» образовательной программы.

Входные требования к дисциплине основываются на теоретических знаниях и практических навыках, приобретённых студентами в процессе обучения на 1 - 4 курсах. Дисциплина основывается на знаниях, полученных обучаемыми при изучении дисциплины «Основы информационной безопасности».

3. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Курс	Семестр	Общая трудоёмкость (ЗЕ)	Общая трудоёмкость (часы)	Контактная работа			Самостоятельная работа (часы)	Промежуточная аттестация
				Лекции (часы)	Лабораторныеработы (часы)	Практические занятия (часы)		
4	8	3	108	32	-	16	60	ЗаО

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

№ и наименование модуля	Контактная работа			Самостоятельная работа	Формы текущего контроля
	Лекции (часы)	Лабораторныеработы (часы)	Практические занятия (часы)		
1. Современная постановка проблемы защиты информации в телекоммуникационных системах и устройствах	6	-	2	6	Устный опрос
2. Требования по защите информации к телекоммуникационным системам и устройствам	4	-	2	6	Устный опрос
3. Архитектура защиты информации в соответствии с базовой эталонной моделью взаимодействия открытых систем	2	-	2	4	Устный опрос

№ и наименование модуля	Контактная работа			Самостоятельная работа	Формы текущего контроля
	Лекции (часы)	Лабораторныер аботы (часы)	Практические занятия (часы)		
4. Криптографические методы защиты информации в телекоммуникационны х системах	8	-	6	14	Устный опрос Контроль выполнения индивидуального задания
5. Защита от несанкционированного доступа и модели безопасности компьютерных систем	6	-	4	14	Устный опрос Контроль выполнения индивидуального задания
6. Защищенные протоколы стека TCP/IP	6	-	4	16	Устный опрос, Защита индивидуальных заданий

4.1. Лекционные занятия

№ модуля дисциплины	№ лекции	Объем занятий (часы)	Краткое содержание
1	1	2	Взаимосвязь современных понятий в области защиты информации
	2	2	Модели угроз информационным технологиям
	3	2	Риск ориентированный подход к обеспечению безопасности телекоммуникационных систем
2	4	2	Система нормативных документов по защите информации. Основные отечественные, зарубежные и международные документы
	5	2	Формирование требований по защите информации к телекоммуникационным устройствам на примере требований к средствам криптографической защиты информации
3	6	2	Архитектура защиты информации в соответствии с базовой эталонной моделью взаимодействия открытых систем
4	7	3	Основные понятия криптографии. Симметричные криптографические алгоритмы. Алгоритмы Магма и AES.
	8	1	Криптографические алгоритмы хеширования. Алгоритм Стрибог.
	9	2	Ассиметричные криптографические алгоритмы. Алгоритм RSA. Электронная цифровая подпись.

№ модуля дисциплины	№ лекции	Объем занятий (часы)	Краткое содержание
	10	2	Инфраструктура открытых ключей.
5	11	2	Введение в управление доступом. Понятия идентификации и аутентификации. Дискреционное и мандатное управление доступом. Понятие доверенный вычислительной среды.
	12	3	Модели безопасности вычислительных систем. Субъектно-объектная модель безопасности вычислительных систем. Доверенная загрузка.
	13	1	Современные средства защиты от несанкционированного доступа.
6	14	1	Стек протоколов TCP/IP и защищенные протоколы в этом стеке.
	15	2	Протокол IPSec.
	16	3	Протокол TLS.

4.2. Практические занятия

№ модуля дисциплины	№ практического занятия	Объем занятий (часы)	Наименование занятия
1	1	2	Анализ рисков информационной безопасности и разработка модели угроз
2	2	2	Определение исходного уровня защищённости телекоммуникационной системы
3	3	2	Исследование защищённости сетевых протоколов с использованием средств анализа сетевого трафика
4	4	2	Симметричные криптографические алгоритмы
	5	2	Электронная цифровая подпись
	6	2	Использование средства шифрования GnuPG для формирования инфраструктуры доверия
5	7	2	Доверенная загрузка вычислительных средств
6	8	2	Использование средств шифрования сетевого трафика

4.3. Лабораторные работы

Не предусмотрены.

4.4. Самостоятельная работа студентов

№ модуля дисциплины	Объем занятий (часы)	Вид СРС
1	2	Подготовка к практическим занятиям «Изучение критериев оценки безопасности информационных технологий»
	2	Подготовка к устному опросу
	2	Подготовка к практическим занятиям «Изучение методик оценки рисков в области информационных технологий»
2	2	Подготовка к практическим занятиям «Изучение нормативных документов в области безопасности информационных технологий»
	2	Подготовка к устному опросу
	2	Подготовка к практическим занятиям «Разработка требований по защите информации к криптографическим средствам защиты информации в составе телекоммуникационного устройства»
3	2	Подготовка к практическим занятиям «Изучение архитектуры защиты информации в соответствии с базовой эталонной моделью взаимодействия открытых систем»
	2	Подготовка к устному опросу
4	14	Выполнение индивидуального задания
	2	Подготовка к устному опросу
5	12	Выполнение индивидуального задания
	2	Подготовка к устному опросу
6	14	Выполнение индивидуального задания
	2	Подготовка к устному опросу

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// URL: ,http://orioks.miet.ru/):

Модуль 1 «Современная постановка проблемы защиты информации в телекоммуникационных системах и устройствах»

Для выполнения СРС по теме «Изучение критериев оценки безопасности информационных технологий» представлены в ОРИОКС (http://orioks.miet.ru/) в разделе ресурсы по дисциплине, Модуль 1:

✓ Руководящий документ. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель, 2002;
✓ ГОСТ Р 51275-99 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.
✓ ГОСТ Р 51898-2002 Аспекты безопасности. Правила включения в стандарты.

Для выполнения СРС по теме «Изучение методик оценки рисков в области информационных технологий» представлены в ОРИОКС (http://orioks.miet.ru/) в разделе ресурсы по дисциплине, Модуль 1:
✓ Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, 2008;
✓ Статья А.В. Шарамок О методе разработки модели источника угроз/ Вопросы защиты информации, № 1, 2013
✓ Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, 2008.
✓ ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.

Модуль 2 «Требования по защите информации к телекоммуникационным системам и устройствам»

Для выполнения СРС по теме «Изучение нормативных документов в области безопасности информационных технологий» представлены в ОРИОКС (http://orioks.miet.ru/) в разделе ресурсы по дисциплине, Модуль 2:
✓ Перечень технической документации, национальных стандартов и методических документов, необходимых для выполнения работ и оказания услуг, установленных Положением о лицензировании деятельности по технической защите конфиденциальной информации, утвержденным постановлением Правительства Российской Федерации от 3 февраля 2012 г. № 79.

Для выполнения СРС по теме «Разработка требований по защите информации к криптографическим средствам защиты информации в составе телекоммуникационного устройства» представлены в ОРИОКС (http://orioks.miet.ru/) в разделе ресурсы по дисциплине, Модуль 2:
✓ Стандарт FIPS-140-2, Security Requirements For Cryptographic Modules, NIST 2001.
✓ Стандарт FIPS-140-3, Security Requirements For Cryptographic Modules, NIST 2019.
✓ Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей;

Модуль 3 «Архитектура защиты информации в соответствии с базовой эталонной моделью взаимодействия открытых систем»

Для выполнения СРС по теме «Разработка требований по защите информации к криптографическим средствам защиты информации в составе телекоммуникационного устройства» представлены в ОРИОКС (http://orioks.miet.ru/) в разделе ресурсы по дисциплине, Модуль 1:
✓ ГОСТ Р ИСО/МЭК 7498-1-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель.

✓ ГОСТ Р ИСО/МЭК 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации.

Модуль 4 «Криптографические методы защиты информации в телекоммуникационных системах»

Для выполнения СРС по теме индивидуального заданиянеобходимо использовать материалы из профессиональных баз данных и баз знаний, представленных в разделе 7 настоящей программы.

Модуль 5 «Защита от несанкционированного доступа и модели безопасности компьютерных систем»

Для выполнения СРС по теме индивидуального заданиянеобходимо использовать материалы из профессиональных баз данных и баз знаний, представленных в разделе 7 настоящей программы.

Модуль 6 «Защищенные протоколы стека TCP/IP»

Для выполнения СРС по теме индивидуального заданиянеобходимо использовать материалы из профессиональных баз данных и баз знаний, представленных в разделе 7 настоящей программы.

6. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ

Литература

1. Галатенко В.А.Основы информационной безопасности : Учеб. пособие. - 2-е изд. - М. : ИНТУИТ, 2016. - 266 с. - URL: https://e.lanbook.com/book/100295 (дата обращения: 21.12.2020). - ISBN 978-5-94774-821-5

2. Бутакова Н.Г. Криптографические методы и средства защиты информации : Учеб. пособие / Н.Г. Бутакова, Н.В. Федоров. - СПб. : ИЦ "Интермедия", 2017. - 384 с. - ISBN 978-5-4383-0135-6

3. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками : Учеб. пособие / П.Н. Девянин. - М. : Горячая линия-Телеком, 2012. - 320 с. - URL: https://e.lanbook.com/book/5150 (дата обращения: 21.12.2020). - ISBN 978-5-9912-0147-6.

4. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам: Учеб. пособие / Под ред. А.А. Шелупанова, С.Л. Груздева, Ю.С. Нахаева. - [2-е изд., стер.]. - М. : Горячая линия-Телеком, 2012. - 550 с. - ISBN 978-5-9912-0257-2:1306-80.

Нормативная литература

1. ГОСТ Р 51898 – 2002 Аспекты безопасности. Правила включения в стандарты = Safetyaspects. Guidelinesfortheirinclusioninstandards: Национальный стандарт РФ :Введ. 01.01.2003. - М.: Стандартинформ, 2018. - URL: https://docs.cntd.ru/document/1200030314 (дата обращения: 21.12.2020).

2. Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий / Гостехкомиссия России. - URL:

https://docs.cntd.ru/document/456058353?marker=2CBO408&section=text (дата обращения: 21.12.2020). - Режим доступа: по заказу демонстрации.
3. ГОСТ Р 51897-2011 Менеджмент риска. Термины и определения: Национальный стандарт РФ :Введ. 01.12.2012. - М.: Стандартинформ, 2019. - URL: https://docs.cntd.ru/document/1200088035 (дата обращения: 21.12.2020).
4. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности: Национальный стандарт РФ :Введ. 01.12.2011. - М.: Стандартинформ, 2011. - URL: https://docs.cntd.ru/document/1200084141 (дата обращения: 21.12.2020).
5. Методика определения актуальных угроз безопасности персональных данных при их обработке и информационных системах персональных данных: Утверждена заместителем директора ФСТЭК России 14 февраля 2008 г. – URL: https://docs.cntd.ru/document/902266674 (дата обращения: 21.12.2020).
6. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения: Национальный стандарт РФ :Введ. 01.02.2008. - М.: Стандартинформ, 2008. - URL: https://docs.cntd.ru/document/1200058320 (дата обращения: 21.12.2020).
7. Р 50.1.056-2005 Техническая защита информации. Основные термины и определения: Рекомендации :Введ. 01.06.2006. - М.: Стандартинформ, 2006. - URL: https://docs.cntd.ru/document/1200044768 (дата обращения: 21.12.2020). - Режим доступа: по заказу демонстрации.
8. ГОСТ Р ИСО/МЭК 7498-1-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель: Государственный стандарт РФ :Введ. 01.01.2000. - М.: Стандартинформ, 2006. - URL: https://docs.cntd.ru/document/1200028699 (дата обращения: 21.12.2020).
9. ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации: Государственный стандарт РФ :Введ. 01.01.2000. - М.: Стандартинформ, 2006. - URL: https://docs.cntd.ru/document/1200007766 (дата обращения: 21.12.2020).
10. ГОСТ 34.10-2018. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи: Межгосударственный стандарт :Введ. 01.06.2019. - М.: Стандартинформ, 2020. - URL: https://docs.cntd.ru/document/1200161706 (дата обращения: 21.12.2020).
11. ГОСТ 34.11-2018. Информационная технология. Криптографическая защита информации. Функция хеширования: Межгосударственный стандарт :Введ. 01.06.2019. - М.: Стандартинформ, 2020. - URL: https://docs.cntd.ru/document/1200161707 (дата обращения: 21.12.2020).
12. ГОСТ 34.12-2018. Информационная технология. Криптографическая защита информации. Блочные шифры: Межгосударственный стандарт :Введ. 01.06.2019. - М.: Стандартинформ, 2020. - URL: https://docs.cntd.ru/document/12001617078 (дата обращения: 21.12.2020).
13. ГОСТ 34.13-2018. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров: Межгосударственный стандарт :Введ. 01.06.2019. – М.: Стандартинформ, 2020. - URL: https://docs.cntd.ru/document/12001617079 (дата обращения: 21.12.2020).

14. Р 1323565.1.030-2018 Информационная технология. Криптографическая защита информации. Использование российских криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.3): Рекомендации по стандартизации: Введ. 0106.2020. – М.: Стандартинформ, 2020. - URL: https://docs.cntd.ru/document/573338314 (дата обращения: 21.12.2020). - Режим доступа: по заказу демонстрации.

Периодические издания

1. Безопасность информационных технологий : научный журнал / ФГАОУ ВО Национальный исследовательский ядерный университет "МИФИ". - Москва : НИЯУ МИФИ, 1994 - . - URL: http://bit.mephi.ru/ (дата обращения: 21.12.2020). - Режим доступа: свободный.
2. Вопросы кибербезопасности : научный журнал / Научно-производственное объединение Эшелон. - Москва : НПО Эшелон, 2013 - . - URL: https://cyberrus.com (дата обращения: 21.12.2020). - Режим доступа: свободный.
3. Вопросы защиты информации : научно-практический журнал / Федеральное государственное унитарное предприятие Научно-технический центр оборонного комплекса "Компас". - Москва : ФГУП НТЦ оборонного комплекса Компас, 1974 - . - URL: http://elibrary.ru/contents.asp?titleid=8588 (дата обращения: 21.12.2020). - Режим доступа: по подписке (2014-2020). - ISSN 2073-2600.
4. Informationsecurity/ информационная безопасность : профессиональное издание. - Москва :Гротек, [2005]. - URL: https://lib.itsec.ru/imag/ (дата обращения: 21.12.2020). - Режим доступа: свободный.

7. ПЕРЕЧЕНЬ ПРОФЕССИОНАЛЬНЫХБАЗ ДАННЫХ, ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ

1. eLIBRARY.RU: Научная электронная библиотека: сайт. - Москва, 2000 -. - URL: https://www.elibrary.ru/defaultx.asp (дата обращения: 21.12.2020). - Режим доступа: для зарегистрированных пользователей.
2. Росстандарт: Стандарты и регламенты: сайт / Федеральное агентство по техническому регулированию и метрологии. – Москва, 2020. - URL: https://www.rst.gov.ru/portal/gost/home/standarts (дата обращения:21.12.2020).
3. NIST :[Раздел по безопасности Лаборатории информационных технологий Национального института по стандартизации США]: [сайт]. –USA, 2020. -Англ. яз. - URL: https://www.nist.gov/cybersecurity(дата обращения:25.12.2020).
4. NIST :[Каракас документов по информационной безопасности Национального института по стандартизации США] : [сайт]. –USA, 2020. -Англ. яз. - URL: https://www.nist.gov/cyberframework (дата обращения:21.12.2020).
5. ISACA : Information Systems Audit and Control Association : [сайт]. – 2020. - Англ. яз. - URL: https://www.isaca.org/ (датаобращения:21.12.2020).
6. TCG:[сайт]. – 2020. - Англ. яз. -URL: https://trustedcomputinggroup.org/ (дата обращения:21.12.2020).
7. IEEE:[сайт]. – 2020. - Англ. яз. -URL: http://www.ieee-security.org/ (дата обращения 25.12.2020).

8. NIST :[База данных уязвимостей продуктов информационной технологии Национального института по стандартизации США] : [сайт]. –USA, 2020. -Англ. яз. – URL: https://nvd.nist.gov/vuln (дата обращения:21.12.2020).
9. IBM :[Академия безопасности IBM]: [сайт]. – 2020. - Англ. яз. - URL: https://www.securitylearningacademy.com/ (дата обращения 21.12.2020).
10. Microsoft[Библиотека материалов по информационной безопасности Microsoft] :[сайт]. – 2020. - Англ. яз. - URL: https://www.microsoft.com/en-us/security/content-library/ (дата обращения:21.12.2020).

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В ходе реализации обучения используется смешанное обучение 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.

Для взаимодействия студентов с преподавателем используются сервисы обратной связи: раздел ОРИОКС «Домашние задания», «Портфолио», «Опрос студентов»и электронная почта.

В процессе обучения при проведении занятий и для самостоятельной работы используются внутренние электронные ресурсы в формах внутренних онлайн-курсов и тестирования в ОРИОКС.

При проведении занятий и для самостоятельной работы используются внешние электронные ресурсы в формах: внешних онлайн баз данных и баз знаний:

- Сайт ФСТЭК России. Банк данных угроз безопасности информации ФСТЭК России: сайт. – URL: https://bdu.fstec.ru/threat (дата обращения 25.11.2020)
- Сайт NIST. Раздел по безопасности Лаборатории информационных технологий Национального института по стандартизации США: сайт. – URL: https://www.nist.gov/cybersecurity (дата обращения 25.11.2020)
- Сайт NIST. Каркас документов по информационной безопасности Национального института по стандартизации США: сайт. – URL: https://www.nist.gov/cyberframework (дата обращения 25.11.2020)
- Сайт (ISC)². InternationalInformationSystemSecurityCertificationConsortium (ISC)² - Консорциум сертификации по безопасности информационных систем: сайт. – URL: https://www.isc2.org/ (дата обращения 25.11.2020)
- Сайт ISACA. InformationSystemsAuditandControlAssociation (ISACA) Ассоциация по аудиту и управлению информационными системами: сайт. – URL: https://www.isaca.org/ (дата обращения 25.11.2020)
- Сайт TCG. Консорциум TrustedComputingGroup (TCG) Группа по доверенным вычислениям: сайт. – URL: https://trustedcomputinggroup.org/ (дата обращения 25.11.2020)
- Сайт IEEE. Технический комитет IEEE по безопасности и приватности: сайт. – URL: http://www.ieee-security.org/ (дата обращения 25.11.2020)

- Сайт NIST. База данных уязвимостей продуктов информационной технологии Национального института по стандартизации США: сайт. – URL: https://nvd.nist.gov/vuln (дата обращения 25.11.2020)

- Сайт компании OffensiveSecurity. База данных уязвимостей продуктов информационной технологии: сайт. – URL: https://www.exploit-db.com/ (дата обращения 25.11.2020)

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	Моноблок Dell Inspirion 3227(IntelCorei3-713U) с беспроводной клавиатурой и мышью.	LibreOffice Интернет браузер. Sumatra pdf . WireShark. Kleopatra, версия Gpg4win. Code::Blocks. Far Manager. GostCrypt. OpenVPN. Oracle VM VirtualBox.
Помещение для самостоятельной работы обучающихся	Компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду МИЭТ	Операционнаясистема Microsoft Windows от 7 версииивыше, Microsoft Office Professional Plu sили Open Office, браузер (Firefox, Google Crome); Acrobat reader DC

10. ФОНДЫ ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕРКИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ/ПОДКОМПЕТЕНЦИЙ

1. ФОС по подкомпетенции**ПК-7.БТС** «Администрирование средств 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

11.1. Особенности организации процесса обучения

Дисциплина предусматривает посещение 100 % аудиторных занятий студентами, в случае прогула студент отвечает на вопросы по пропущенному занятию.

Для подготовки к устному опросу студент осуществляет закрепление и расширение знаний общей специфической тематикой. Рекомендуется проводить подготовку по одному либо нескольким источникам и формировать краткий конспект по обозреваемой теме.

В рамках изучения дисциплины учащиеся должны выполнить индивидуальное задание (проект). Примерные тематики заданийвыдаются преподавателем. Результатом выполнения задания является пояснительная записка и материалы доклада. При необходимости дополнительно предоставляется макет созданного технического решения. Как правила макет представляется в виде образов виртуальных машин с настроенным или разработанным программным обеспечением. При необходимости макет может содержать аппаратные компоненты.

Результаты индивидуального задания (проекта) защищаются в виде публичного доклада.

График выполнения задания представлен в таблице ниже.

№	Содержание пункта	Дата завершения
1	Получение темы индивидуального здания	до 4 недели
2	Предоставление на проверку и уточнение индивидуального задания.	до 10 недели
3	Предоставление преподавателю на проверку черновой версии результатов выполнения индивидуального задания	до 12 недели
4	Получение замечаний по черновой версии индивидуального задания	до 14 недели
5	Исправление результатов индивидуального задания по замечаниям преподавателя и предоставление окончательного отчета по индивидуальному заданию	до 15 недели
6	Защита индивидуальных заданий	16-17 неделя

Требования к содержанию отчетных материалов по выполнению индивидуального задания:

- Индивидуальное задание;
- Пояснительная записка по выполнению индивидуального задания (не менее 15 стр.);
- Слайды для доклада по индивидуальному заданию (не менее 20 слайдов);
- Макет созданного технического решения.

Индивидуальное задание должно содержать:

- название темы;
- назначение выполняемой работы;
- требования к создаваемому техническому решению (состав, технические характеристики и др. при необходимости);

- требования к содержанию пояснительной записки (план проспект пояснительной записки);

- требования к содержанию слайдов доклада.

В пояснительной записке должна содержаться информация об исследовании вопроса по тематике индивидуального задания, формулировки требований к индивидуальному заданию, разработка решения по тематике индивидуального задания и доказательство корректности этого решения (тестирование).

11.2. Система контроля и оценивания

Для оценки успеваемости студентов по дисциплине используется накопительная балльная система. Баллами оцениваютсявыполнение каждого контрольного мероприятия в семестре.

Баллами оцениваются: выполнение каждого контрольного мероприятия в семестре (в сумме 100 баллов), активность в семестре (в сумме 70 баллов) и зачет с оценкой (30 баллов).

В течение семестра основные контрольные мероприятия проводятся на практических занятиях. За контрольное мероприятие в рамках практического занятия учащийся может получить от 0 до 6 баллов. Контрольным мероприятием в течение семестра является защита индивидуального задания. По результатам выполнения и защиты индивидуального задания учащийся может получить от 0 до 22 баллов.

По сумме баллов выставляется итоговая оценка. Структура и график контрольных мероприятий доступен в ОРИОКС// URL: http://orioks.miet.ru/.

РАЗРАБОТЧИК:

Доценткафедры ТКС, к.т.н._____/А.В.Шарамок/

Рабочая программа дисциплины «Безопасность телекоммуникационных систем» по направлению подготовки 11.03.02 «Инфокоммуникационные технологии и системы связи», направленности (профилю) «Сети и системы инфокоммуникаций» разработана на кафедре ТКС и утверждена на заседании кафедры 25.12 2020 года, протокол № 6

Заведующий кафедрой ТКС _____/А.А. Бахтин /

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 /