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
«28» 12 2020 г.
М.П.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

«Обеспечение информационной безопасности в телекоммуникационных системах и устройствах»

Направление подготовки – 11.04.02 «Инфокоммуникационные технологии и системы связи»
Направленность (профиль) – «Информационные сети и телекоммуникации»

Москва 2020

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ

Дисциплина участвует в формировании следующих компетенций образовательных программ:

Компетенции ОП	**Подкомпетенции, формируемые в дисциплине**	**Индикаторы достижения компетенций**
ОПК-1 Способен представлять современную научную картину мира, выявлять естественнонаучную сущность проблем своей профессиональной деятельности, определять пути их решения и оценивать эффективность сделанного выбора	ОПК-1.ОИБТКСиУ Способен формулировать требования по информационной безопасности и организовывать эксплуатацию и контроль работы защищенной работы инфокоммуникационной системы и сервисов	**Знания:** уязвимых мест инфокоммуникационных систем и соответствующих сервисов в плане возможных нарушений информационной и функциональной безопасности. Модели взаимодействия открытых систем ISO/OSI. Международных, федеральных, ведомственных стандартов и рекомендаций, устанавливающих требования к методам мониторинга и контроля функционирования инфокоммуникационных систем и соответствующих сервисов, к их качеству. **Умения:** оценивать наличие и степень нарушений требований обеспечения информационной и функциональной безопасности инфокоммуникационных систем и соответствующих сервисов. Формулировать критерии оценки функционирования инфокоммуникационных систем и сервисов. **Опыт деятельности:** подключать и настраивать современные средства защиты информации; использовать средства криптографической защиты информации (шифрования и цифровой подписи); использовать средства построения виртуальных частных сетей для предотвращения атак.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина входит в обязательную часть Блока 1 «Дисциплины (модули)» образовательной программы.

Входные требования к дисциплине основываются на теоретических знаниях и практических навыках, приобретённых студентами в процессе обучения в бакалавриате и 1 семестре обучения в магистратуре.

3. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Курс	Семестр	Общая трудоёмкость (ЗЕ)	Общая трудоёмкость (часы)	Контактная работа			Самостоятельная работа (часы)	Промежуточная аттестация
				Лекции (часы)	Лабораторные работы (часы)	Практические занятия (часы)		
1	2	3	108	-	32	16	60	ЗаО

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

№ и наименование модуля	Контактная работа			Самостоятельная работа	Формы текущего контроля
	Лекции (часы)	Лабораторные работы (часы)	Практические занятия (часы)		
1. Архитектура защиты информации	-	8	2	10	Устный опрос Защита лабораторных работ
2. Современная постановка задачи защиты информации	-	4	4	10	Устный опрос Защита лабораторной работы
3. Введение в криптографическую защиту информации		12	4	10	Устный опрос

№ и наименование модуля	Контактная работа			Самостоятельная работа	Формы текущего контроля
	Лекции (часы)	Лабораторные работы (часы)	Практические занятия (часы)		
4. Введение в управление доступом		8	2	10	Устный опрос Защита лабораторных работ
5. Модели безопасности компьютерных систем		-	4	20	Устный опрос Защита индивидуальных заданий

4.1. Лекционные занятия

Не предусмотрены

4.2. Практические занятия

№ модуля дисциплины	№ практического занятия	Объем занятий (часы)	Наименование занятия
1	1	2	Архитектура защиты информации в соответствии с базовой эталонной моделью взаимодействия открытых систем
2	2	2	Взаимосвязь современных понятий в области защиты информации
	3	2	Риск ориентированный подход к обеспечению безопасности телекоммуникационных систем
3	4	2	Основные понятия криптографии. Симметричные криптографические алгоритмы. Алгоритмы Магма и AES. Алгоритм Стрибог
	5	2	Ассиметричные криптографические алгоритмы. Алгоритм RSA. Электронная цифровая подпись
4	6	2	Введение в управление доступом. Понятия идентификации и аутентификации. Дискреционное и мандатное управление доступом.
5	7	2	Модели безопасности вычислительных систем.
	8	2	Субъектно-объектная модель безопасности вычислительных систем. Доверенная загрузка

4.3. Лабораторные работы

№ модуля дисциплины	№ лабораторной работы	Объем занятий (часы)	Наименование работы
1	1	4	Работа со средствами виртуализации Virtual Box и сетевым анализатором WireShark
	2	4	Анализ защищённых протоколов из стека TCP/IP
2	3	4	Использование инструментальных средств для анализа рисков информационной безопасности
3	4	4	Отладка программной реализации криптографического алгоритма Магма
	5	4	Прозрачное шифрование диска с использованием средства GostCrypt
	6	4	Построение сети доверия с использованием OpenPGP и средства средство шифрования Kleopatra
4	7	4	Удаленный доступ к сетевым ресурсам с использованием средства OpenVPN
	8	4	Управление доступом с использованием технологии LDAP

4.4. Самостоятельная работа студентов

№ модуля дисциплины	Объем занятий (часы)	Вид СРС
1	2	Подготовка к практическим занятиям «Изучение базовой эталонной модели взаимодействия открытых систем»
	2	Подготовка к практическим занятиям «Изучение архитектуры защиты информации в соответствии с базовой эталонной моделью взаимодействия открытых систем»
	6	Подготовка к выполнению и защите лабораторных работ 1, 2
2	3	Подготовка к практическим занятиям «Изучение нормативных документов в области безопасности информационных технологий»
	3	Подготовка к практическим занятиям «Изучение требований по защите информации к криптографическим средствам защиты информации»
	4	Подготовка к выполнению и защите лабораторной работы 3
3	2	Подготовка к практическим занятиям «Изучение современных блочных шифров»
	2	Подготовка к практическим занятиям «Изучение современных

№ модуля дисциплины	Объем занятий (часы)	Вид СРС
		асимметричных шифров»
	6	Подготовка к выполнению и защите лабораторных работ 4-6
4	3	Подготовка к практическим занятиям «Изучение протоколов IPSec и TLS»
	3	Подготовка к практическим занятиям «Изучение архитектуры и принципов технологии LDAP»
	4	Подготовка к выполнению и защите лабораторных работ 7-8
5	20	Выполнение индивидуальных проектов

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 «Архитектура защиты информации»

Для выполнения СРС по теме «Изучение базовой эталонной моделью взаимодействия открытых систем» 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.

Для выполнения СРС по теме «Изучение архитектуры защиты информации в соответствии с базовой эталонной моделью взаимодействия открытых систем» представлены в ОРИОКС (http://orioks.miet.ru/) в разделе ресурсы по дисциплине, Модуль 1:

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

Модуль 2 «Современная постановка задачи защиты информации»

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:

✓ 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.

✓ ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.

✓ Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, 2008.
✓ Статья Шарамок А.В. 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.

Для выполнения СРС по теме «Изучение требований по защите информации к криптографическим средствам защиты информации» представлены в ОРИОКС (http://orioks.miet.ru/) в разделе ресурсы по дисциплине, Модуль 1:
✓ 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.
✓ Р 1323565.1.012-2017 Рекомендации по стандартизации. Информационная технология. Криптографическая защита информации. Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации

Модуль 3 «Введение в криптографическую защиту информации»

Для выполнения СРС по теме «Изучение современных блочных шифров» представлены в ОРИОКС (http://orioks.miet.ru/) в разделе ресурсы по дисциплине, Модуль 3:
✓ К. Шеннон «Работы по теории информации и кибернетике», М., ИЛ, 1963, с. 333-369.
✓ ГОСТ Р 34.13–2015 «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров».
✓ ГОСТ Р 34.12–2015 «Информационная технология. Криптографическая защита информации. Блочные шифры».
✓ ГОСТ Р 34.11–2012 «Информационная технология. Криптографическая защита информации. Функция хэширования».
✓ FIPS 197 Advanced Encryption Standard (AES), November 2001

Для выполнения СРС по теме «Изучение современных асимметричных шифров» представлены в ОРИОКС (http://orioks.miet.ru/) в разделе ресурсы по дисциплине, Модуль 3:
✓ ГОСТ Р 34.10–2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»
✓ Rivest, R.; Shamir, A.; Adleman, L. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems" Communications of the ACM. 21 (2), February 1978.
✓ FIPS 186-4 Digital Signature Standard (DSS), July 2013

Модуль 4 «Введение в управление доступом»

Для выполнения СРС по теме «Изучение протоколов IPSec и TLS» представлены в ОРИОКС (http://orioks.miet.ru/) в разделе ресурсы по дисциплине, Модуль 3:
✓ Р 1323565.1.020-2020 «Информационная технология. Криптографическая защита информации. Использование российских криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.2)».
✓ Р 1323565.1.034–2020 «Информационная технология. Криптографическая защита информации. Протокол бР 1323565.1.030-2020 «Информационная технология.

Криптографическая защита информации. Использование криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.3)».

✓ Р 1323565.1.034–2020 «Информационная технология. Криптографическая защита информации. Протокол безопасности сетевого уровня».

Для выполнения СРС по теме «Изучение архитектуры и принципов технологии LDAP» представлены в ОРИОКС (http://orioks.miet.ru/) в разделе ресурсы по дисциплине, Модуль 3:

✓ Understanding LDAP - Design and Implementation. An IBM Redbooks publication. Published 16 June 2004, updated 19 July 2006.

Модуль 5 «Модели безопасности компьютерных систем»

Для выполнения СРС по теме «Выполнение индивидуальных проектов» необходимо использовать материалы из профессиональных баз данных и баз знаний, представленных в разделе 7 настоящей программы.

Примерные тематики индивидуальных проектов:

Оценка риска с использованием методики ГОСТ Р ИСО/МЭК 31010-2011.

Оценка риска с использованием методики Национального института стандартов и технологий США.

Концепция обеспечения доверия к информационным технологиям в соответствии с методикой ГОСТ Р 54581-2011.

Методы обеспечения доверия к информационным технологиям в соответствии с ГОСТ Р 54582-2011.

Анализ методов обеспечения доверия к информационным технологиям в соответствии с ГОСТ Р 54583-2011.

Разработка модели угроз для ЛВС кафедры ТКС в соответствии с ГОСТ Р 57628—2017.

Анализ уязвимостей устройств и систем IoT в соответствии с ГОСТ Р 57628—2017.

Разработка модели угроз для устройств IoT в соответствии с ГОСТ Р 56545 -2015 и ГОСТ Р 56546 -2015.

Реализация механизмов контроля загрузки в операционной системе Linux.

Шифрование электронной почты по спецификации S/MIME с использованием стандарта PGP.

Шифрование электронной почты по спецификации S/MIME с использованием стандарта PKCS-7.

Управление криптографическими ключами в системе PGP (Kleopatra, GPA и др.).

Обеспечение доверенной загрузки вычислительных средств общего назначения с использованием Trusted Platform Module.

Обеспечение аутентификации сетевых устройств с использованием инфраструктура открытых ключей PKI.

Настройка управления доступом в локальной сети кафедры ТКС с использованием свободно распространяемого ПО и протокола LDAP.

Создание сервера генерации цифровых сертификатов X.509 с использованием библиотеки SSH.

Создание удостоверяющего центра с использованием свободно распространяемого программного обеспечения.

6. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ

Литература

1. Галатенко В.А. Стандарты информационной безопасности / В.А. Галатенко. - 2-е изд. - М. : ИНТУИТ, 2016. - 418. - URL: https://e.lanbook.com/book/100511 (дата обращения: 21.12.2020). - ISBN 5-9556-0053-1.
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 : 834-20.
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.

Дополнительная литература

1. Основы криптографии для экономистов: Учеб. пособие / С.П. Панасенко, В.П. Батура; Под ред. Л.Г. Гагариной. - М.:Финансы и статистика, 2005. - 176 с. - ISBN 5-279-02938-6:96-31.

Нормативная литература

1. ГОСТ Р 51898 – 2002 Аспекты безопасности. Правила включения в стандарты. Введен 01.01.20103. − М.: Стандартинформ, 2018 − URL: https://docs.cntd.ru/document/1200030314 (дата обращения 21.12.2020).
2. РД. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Введен приказом Гостехкомиссии России от 19.06.02 г. № 187. − М., 2001 − URL: https://fstec.ru/component/attachments/download/293 (дата обращения 21.12.2020).
3. ГОСТ Р 51897-2011/Руководство ИСО 73:2009. Менеджмент риска. Термины и определения. Введен 01.12.2020. − М.: Стандартинформ, 2019. − URL: https://docs.cntd.ru/document/1200088035 (дата обращения 21.12.2020).
4. ГОСТ Р ИСО/МЭК 31000-2010 Менеджмент риска. Принципы и руководство. Введен 01.09.2011. − М.: Стандартинформ, 2018 − URL: https://docs.cntd.ru/document/1200089640 (дата обращения 21.12.2020).
5. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. Введен 01.12.2011. − М.: Стандартинформ, 2011 − URL: https://docs.cntd.ru/document/1200084141 (дата обращения 21.12.2020).
6. Методика определения актуальных угроз безопасности персональных данных при их обработке и информационных системах персональных данных. Утв. 14 февраля 2008 г. − М., 2008 − URL: https://fstec.ru/component/attachments/download/290 (дата обращения 21.12.2020).

7. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. Введен 01.02.2008. − М.: Стандартинформ, 2008 − URL: https://docs.cntd.ru/document/1200058320 (дата обращения 21.12.2020).
8. ГОСТ Р ИСО/МЭК 7498-1-99 Информационная технология (ИТ). Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель. Введен 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 (ИТ). Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен 01.01.2000. − М.: ИПК Издательство стандартов, 1999. − 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. Введен 01.09.2019. − URL: https://docs.cntd.ru/document/1200161706 (дата обращения 21.12.2020).
11. ГОСТ 34.11-2018. Информационная технология. Криптографическая защита информации. Функция хеширования. Введен 01.06.2019. − URL: https://docs.cntd.ru/document/1200161707 (дата обращения 21.12.2020).
12. ГОСТ 34.12-2018. Информационная технология. Криптографическая защита информации. Блочные шифры. Введен 01.06.2019. − URL: https://docs.cntd.ru/document/1200161708 (дата обращения 21.12.2020).
13. ГОСТ 34.13-2018. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров. Введен 01.06.2019. − URL: https://docs.cntd.ru/document/1200161709 (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). Введен 01.06.2020. – URL: https://docs.cntd.ru/document/573338314 (дата обращения 21.12.2020).

Периодические издания

1. Вопросы Кибербезопасности : научный журнал / Научно-производственное объединение Эшелон. - Москва : НПО Эшелон, 2013 - . - URL: https://cyberrus.com (дата обращения: 21.12.2020). - Режим доступа: свободный. - ISSN 2311-3456.
2. Information Security Информационная безопасность: журнал сайт. – URL: https://lib.itsec.ru/articles2/allpubliks (дата обращения 21.12.2020). - Режим доступа: свободный.

7. ПЕРЕЧЕНЬ ПРОФЕССИОНАЛЬНЫХ БАЗ ДАННЫХ, ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ

1. ФГУП ВНИИФТРИ: научно-исследовательский институт физико-технических и радиотехнических измерений: сайт. – URL: http://www.vniiftri.ru (дата обращения: 21.12.2020). - Режим доступа: свободный.
2. Scopus: экспертно кураторская база данных рефератов и цитат: сайт. – Elsevier, 2020. - URL: http://www.scopus.com (дата обращения: 21.12.2020).
3. 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.
4. IEEE/IET Electronic Library (IEL) [Электронный ресурс] = IEEE Xplore: Электронная библиотека. - USA; UK, 1998-. - URL: https://ieeexplore.ieee.org/Xplore/home.jsp (дата обращения: 21.12.2020). - Режим доступа: из локальной сети НИУ МИЭТ в рамках проекта "Национальная подписка"
5. Международный союз электросвязи: специализированное учреждение ООН: сайт. – URL: https://www.itu.int/ru/Pages/default.aspx (дата обращения: 21.12.2020). - Режим доступа: свободный.
6. 3GPP: Партнерский проект 3-го поколения: сайт. – URL: https://www.3gpp.org/ (дата обращения: 21.12.2020). - Режим доступа: свободный.

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 22.12.2020)
- Сайт NIST. Раздел по безопасности Лаборатории информационных технологий Национального института по стандартизации США: сайт. – URL: https://www.nist.gov/cybersecurity (дата обращения 22.12.2020)
- Сайт NIST. Каркас документов по информационной безопасности Национального института по стандартизации США: сайт. – URL: https://www.nist.gov/cyberframework (дата обращения 22.12.2020)

- Сайт (ISC)². International Information System Security Certification Consortium (ISC)² - Консорциум сертификации по безопасности информационных систем: сайт. – URL: https://www.isc2.org/ (дата обращения 22.12.2020)

- Сайт ISACA. Information Systems Audit and Control Association (ISACA) Ассоциация по аудиту и управлению информационными системами: сайт. – URL: https://www.isaca.org/ (дата обращения 22.12.2020)

- Сайт TCG. Консорциум Trusted Computing Group (TCG) Группа по доверенным вычислениям: сайт. – URL: https://trustedcomputinggroup.org/ (дата обращения 22.11.2020)

- Сайт IEEE. Технический комитет IEEE по безопасности и приватности: сайт. – URL: http://www.ieee-security.org/ (дата обращения 22.12.2020)

- Сайт NIST. База данных уязвимостей продуктов информационной технологии Национального института по стандартизации США: сайт. – URL: https://nvd.nist.gov/vuln (дата обращения 22.12.2020)

- Сайт компании Offensive Security. База данных уязвимостей продуктов информационной технологии: сайт. – URL: https://www.exploit-db.com/ (дата обращения 22.12.2020)

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(Intel Core i3-713U) с беспроводной клавиатурой и мышью	LibreOffice Интернет браузер Sumatra pdf WireShark Kleopatra, Code::Blocks Far Manager GostCrypt OpenVPN Oracle VM VirtualBox
Учебная аудитория	Моноблок Dell Inspirion 3227(Intel Core i3-713U) с беспроводной клавиатурой и мышью	LibreOffice Интернет браузер Sumatra pdf WireShark Kleopatra, Code::Blocks Far Manager GostCrypt OpenVPN Oracle VM VirtualBox

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(Intel Core i3-713U) с беспроводной клавиатурой и мышью	LibreOffice Интернет браузер Sumatra pdf WireShark Kleopatra, 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	Операционная система Microsoft Windows от 7 версии и выше, Microsoft Office Professional Plus или Open Office, браузер (Firefox, Google Crome); Acrobat reader DC

10. ФОНДЫ ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕРКИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ/ПОДКОМПЕТЕНЦИЙ

ФОС по подкомпетенции **ОПК-1.ОИБТКСиУ** «Способен формулировать требования по информационной безопасности и организовывать эксплуатацию и контроль работы защищенной работы инфокоммуникационной системы и сервисов».

Фонд оценочных средств представлен отдельным документом и размещен 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

Для успешной подготовки к семинару студенты должны дома подготовить к занятию 3–4 примера формулировки темы исследования, представленного в монографиях, научных статьях, отчетах. Затем они самостоятельно осуществляют поиск соответствующих источников, определяют актуальность конкретного исследования процессов и явлений, выделяют основные способы доказательства авторами научных работ ценности того, чем они занимаются.

Подготовка к лабораторной работе включает следующие элементы самостоятельной деятельности: четкое представление цели и задач, поставленных в лабораторной работе; выделение навыков умственной, аналитической, научной деятельности, которые станут результатом предстоящей работы. Выработка навыков осуществляется с помощью получения новой информации об изучаемых процессах и с помощью знания о том, в какой степени в данное время студент владеет методами исследовательской деятельности, которыми он станет пользоваться на лабораторном занятии.

Во время подготовки к лабораторным занятиям студенты должны подготовить конспекты, где должны быть четко прописаны цели и задачи выполняемой работы, основные методы и алгоритмы проведения исследования, должна быть проанализирована планируемая к использованию аппаратура и программное обеспечение. Должен быть прописан план выполнения работы с перечислением всех анализируемых характеристики. Допускается использовать один конспект на подгруппу студентов, определенных заранее.

Защита лабораторных работ направлена на систематизацию и закрепление полученных теоретических знаний и практических умений обучающихся. Самостоятельная работа по подготовке к защите лабораторной работы включает в себя:

- изучение конспектов лекций и лабораторной работы, раскрывающих материал, закрепляемый на лабораторной работе;

- повторение учебного материла, полученного при подготовке к лабораторной работе и во время её выполнения;

- анализ проведенных при выполнении лабораторной работы действий и полученных результатов.

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 индивидуальный проект. Примерные тематики индивидуальных проектов представлены в разделе 5. Задание на выполнение индивидуального проекта оформляется в виде индивидуального задания, уточняющего общую тематику индивидуальных проектов.

Результатом выполнения индивидуального проекта 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 проекта защищаются в процессе получения зачета.

График выполнения индивидуальных проектов представлен в таблице ниже.

№	Содержание пункта	Дата завершения
1	Получение темы индивидуального проекта	до 4 недели
2	Предоставление на проверку и уточнение индивидуального задания.	до 10 недели
3	Предоставление преподавателю на проверку черновой версии результатов выполнения индивидуального проекта	до 12 недели
4	Получение замечаний по черновой версии	до 14 недели

	индивидуального проекта	
5	Исправление результатов индивидуального проекта по замечаниям преподавателя и предоставление окончательного отчета по индивидуальному заданию	до 15 недели
6	Защита индивидуальных проектов	16 неделя, зачетная неделя

Требования к содержанию отчетных материалов по выполнению индивидуального проекта:

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

Индивидуальное задание должно содержать:

- название темы индивидуального проекта;
- 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 проекта, формулировки требований к индивидуальному проекту, разработка решения по тематике индивидуального проекта и доказательство корректности этого решения (тестирование).

11.2. Система контроля и оценивания

Для оценки успеваемости студентов по дисциплине используется накопительная балльная система. Баллами оцениваются выполнение 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 течении семестра основные контрольные мероприятия осуществляются на практических занятиях (всего 8 практических занятии). За контрольное мероприятие в рамках практического занятия учащийся может получить от 0 до 6 баллов. Контрольным мероприятием в течении семестра является защита индивидуального проекта. По результатам выполнения и защиты индивидуального проекта 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:

Доцент кафедры ТКС, к.т.н. _____ /А.В. Шарамок/

Рабочая программа дисциплины «Обеспечение информационной безопасности в телекоммуникационных системах и устройствах» по направлению подготовки 11.04.02 «Инфокоммуникационные технологии и системы связи», направленности (профилю) «Информационные сети и телекоммуникации» 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 /