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
_____ А.Г. Балашов
«15» сентября 2025 г.
М.П.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

«Безопасность сетей связи»

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

Москва 2025

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ

Дисциплина участвует в формировании следующих компетенций образовательных программ:

Компетенция ПК-4 «Способен к обеспечению информационной безопасности системного программного обеспечения инфокоммуникационной системы организации» **сформулирована на основе профессионального стандарта 06.026** «Системный администратор информационно-коммуникационных систем».

Обобщенная трудовая функция Е Проектирование модернизации информационно-коммуникационной системы.

Трудовая функция Е/06.7 Разработка дизайна информационно-коммуникационной системы.

Подкомпетенции, формируемые в дисциплине	**Задачи профессиональной деятельности**	**Индикаторы достижения подкомпетенций**
ПК-4.БСС «Способен обеспечивать информационную безопасность инфокоммуникационных систем»	Осуществление разработки отдельных методик контроля и мониторинга функционирования инфокоммуникационных систем и предоставляемых на их основе сервисов. Проведение работы по организации эксплуатации новой сформированной (разработанной) системы автоматизированного мониторинга и контроля функционирования данной инфокоммуникационной системы и сервисов.	**Знания:** уязвимые места инфокоммуникационных систем и соответствующих сервисов в плане возможных нарушений информационной и функциональной безопасности. **Умения:** оценивать наличие и степень нарушений требований обеспечения информационной и функциональной безопасности инфокоммуникационных систем и соответствующих сервисов. **Опыт деятельности:** настраивать средства защиты информации в составе операционных систем; использовать средства тестирования защищенности телекоммуникационных систем; использовать средства автоматизации тестирования защищённости

		телекоммуникационных систем и средства предотвращения атак.

Компетенция ПК-5 «Способен руководить научно-техническими исследованиями по разработке инновационных радиоэлектронных средств» **сформулирована на основе профессионального стандарта 06.048** «Инженер-радиоэлектронщик в области радиотехники и телекоммуникаций»

Обобщенная трудовая функция H Руководство научно-исследовательскими и опытно-конструкторскими работами по разработке и совершенствованию радиоэлектронных средств различного назначения

Трудовая функция H/01.7 Руководство научно-техническими исследованиями по разработке инновационных радиоэлектронных средств.

Подкомпетенции, формируемые в дисциплине	**Задачи профессиональной деятельности**	**Индикаторы достижения подкомпетенций**
ПК-5.БСС Способен организовывать и проводить оценку работоспособности и эффективность применения программно-аппаратных средств защиты информации	Разработка математических, физических и экспериментальных направлений исследований, схемы деления на составные части разрабатываемого радиоэлектронного средства; руководство теоретическими и экспериментальными исследованиями разрабатываемого радиоэлектронного средства; разработка технических заданий для соисполнителей, исполнителей и контроль их выполнения; экспертная оценка предлагаемых исполнителями технических решений, методов и результатов исследований	**Знания**: методов и методики оценки безопасности программно-аппаратных средств защиты информации; методов оценки эффективности политики безопасности, реализованной в программно-аппаратных средствах защиты информации; способов анализа применяемых методов и средств защиты информации на предмет соответствия политике безопасности **Умения**: определять параметры функционирования программно-аппаратных средств защиты информации; разрабатывать методики оценки защищенности программно-аппаратных средств защиты информации; применять разработанные методики оценки защищенности программно-аппаратных средств защиты информации **Опыт деятельности**: в

		настройке и использовании средств тестирования защищенности сетей связи.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

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

Входные требования к дисциплине основываются на теоретических знаниях и практических навыках, приобретённых студентами в процессе обучения в бакалавриате и 1 годе 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)	Практическая подготовка при проведении лабораторных работ (часы)	Практические занятия (часы)		
2	3	4	144	-	40	8	60	Экз (36)

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

№ и наименование модуля	Контактная работа			Самостоятельная работа	Формы текущего контроля
	Лекции (часы)	Практическая подготовка при проведении лабораторных работ (часы)	Практические занятия (часы)		
1. Принципы построения защищенных сетевых протоколов	-	8	2	10	Устный опрос Защита лабораторной работы
2. Защищенные протоколы сетевого уровня	-	12	2	20	Устный опрос Защита лабораторной работы
3. Защищенные протоколы транспортного уровня	-	12	2	20	Устный опрос Защита лабораторной работы
4 Защищенные протоколы систем Интернета вещей	-	8	2	10	Устный опрос Защита лабораторной работы Защита профессионально-ориентированных заданий

4.1. Лекционные занятия

Не предусмотрены

4.2. Практические занятия

№ модуля дисциплины	№ практического занятия	Объем занятий (часы)	Наименование занятия
1	1	2	Принципы построения защищенных сетевых протоколов
2	2	2	Защищенный протокол сетевого уровня IPSec
3	3	2	Защищенные протоколы транспортного уровня TLS и QUIC
4	4	2	Защищенные протоколы систем Интернета вещей

4.3. Практическая подготовка при проведении лабораторных работ

№ модуля дисциплины	№ лабораторной работы	Объем занятий (часы)	Наименование работы
1	1	4	Установка и начальная настройка Kali Linux
	2	4	Настройка сети и сетевых служб в Kali Linux
2	3	4	Настройка безопасности в Kali Linux
	4	4	Продвинутая настройка Kali Linux
	5	4	Создание пакетов и дистрибутивов в Kali Linux
3	6	4	Настройка работы Kali Linux с репозитарием масштаба предприятия
	7	4	Введение проведение расследований с использованием Kali Linux
	8	4	Сканирование уязвимостей с использованием инструмента OWASP ZAP
4	9	4	Реализация атак с использованием уязвимостей службы RPC
	10	4	Реализация ARP-спуфинга с помощью инструментов дистрибутива Kali Linux

4.4. Самостоятельная работа студентов

№ модуля дисциплины	Объем занятий (часы)	Вид СРС
1	5	Подготовка к практическому занятию «Изучение принципов построения защищенных сетевых протоколов»
	5	Выполнение индивидуальных проектов
2	5	Подготовка к практическому занятию «Изучение защищённого протокола сетевого уровня IPSec»
	5	Выполнение индивидуальных проектов
	5	Подготовка к выполнению лабораторных работ
	5	Подготовка к защите лабораторных работ
3	5	Подготовка к практическому занятию «Изучение защищенных протоколов транспортного уровня TLS и QUIC»
	5	Выполнение индивидуальных проектов
	5	Подготовка к выполнению лабораторных работ
	5	Подготовка к защите лабораторных работ

№ модуля дисциплины	Объем занятий (часы)	Вид СРС
4	3	Подготовка к практическому занятию «Изучение защищенных протоколов систем Интернета вещей»
	3	Выполнение индивидуальных проектов
	4	Выполнение профессионально-ориентированных заданий

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 «Принципы построения защищенных сетевых протоколов»

Для выполнения СРС по теме «Изучение принципов построения защищенных сетевых протоколов» 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.

✓ МР 26.2.002-2013 «Использование алгоритмов ГОСТ 28147-89, ГОСТ Р 34.10 и ГОСТ Р 34.11 в криптографических сообщениях формата CMS»;

✓ Р 1323565.1.025–2019 «Информационная технология. Криптографическая защита информации. Форматы сообщений, защищенных криптографическими методами».

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

Модуль 2 «Защищенный протокол сетевого уровня»

Для выполнения СРС по теме «Изучение защищённого протокола сетевого уровня IPSec» представлены в ОРИОКС (http://orioks.miet.ru/) в разделе ресурсы по дисциплине, Модуль 2:

✓ Р 1323565.1.035–2021 «Информационная технология. Криптографическая защита информации. Использование российских криптографических алгоритмов в протоколе защиты информации ESP».

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

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

Модуль 3 «Защищенные протоколы транспортного уровня»

Для выполнения СРС по теме «Изучение защищенных протоколов транспортного уровня TLS и QUIC» 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 1323565.1.030-2020 «Информационная технология. Криптографическая защита информации. Использование криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.3)».

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

Модуль 4 «Защищенные протоколы систем Интернета вещей»

Для выполнения СРС по теме «Изучение защищенных протоколов систем Интернета вещей» представлены в ОРИОКС (http://orioks.miet.ru/) в разделе ресурсы по дисциплине, Модуль 4:

✓ МР 26.4.001-2019 «Протокол защищенного обмена для индустриальных систем (CRISP 1.0)»;

✓ МР 26.4.003-2018 «Криптографические механизмы защищенного взаимодействия контрольных и измерительных устройств»;

✓ МР 26.4.003-2019 «Информационная технология. Криптографическая защита информации. Использование российских криптографических механизмов для реализации обмена данными по протоколу dlms».

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

Примерная тематика индивидуальных проектов:

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

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

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

Создание IPSec шлюза с использованием открытого программного обеспечения ОС Linux.

Создание VPN шлюза с использованием открытого программного обеспечения, ОС Linux и протокола TLS.

Создание VPN шлюза с использованием открытого программного обеспечения, ОС Linux и управления ключами на основе инфраструктуры открытых ключей PKI.

Обеспечение аутентификации сетевых устройств с использованием инфраструктура открытых ключей PKI.

Построение системы криптографической защиты в системах радиодоступа технологий типа WiFi.

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. Поляков, Е. А. Основы информационной безопасности : учебное пособие / Е. А. Поляков. — Нижний Новгород : ННГУ им. Н. И. Лобачевского, 2021. — 71 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/282890 (дата обращения: 27.08.2025). — Режим доступа: для авториз. пользователей.
2. Игнатьева, Е. П. Основы информационной безопасности : учебное пособие / Е. П. Игнатьева. — Иркутск : ИРНИТУ, 2023. — 96 с. — ISBN 978-5-8038-1976-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/497837 (дата обращения: 27.08.2025). — Режим доступа: для авториз. пользователей
3. Шаньгин, Комплексная защита информации в корпоративных системах : учебное пособие / В. Ф. Шаньгин. - Москва : Форум, 2022. - 592 с. - (Высшее образование: Бакалавриат). - URL: https://znanium.com/catalog/product/1843022 (дата обращения: 30.10.2023). - ISBN 978-5-8199-0730-6. - Текст : электронный.
4. Бутакова Н.Г. Криптографические методы и средства защиты информации : Учеб. пособие / Н.Г. Бутакова, Н.В. Федоров. - СПб. : ИЦ "Интермедия", 2020. - 380 с. - URL: https://e.lanbook.com/book/161347 (дата обращения: 23.07.2025). - ISBN 978-5-4383-0210-0.
5. Программно-аппаратные средства обеспечения информационной безопасности : учебное пособие / А. В. Душкин, О. М. Барсуков, Е. В. Кравцов, К. В. Славнов. - Москва : Горячая линия-Телеком, 2018. - 248 с. - URL: https://e.lanbook.com/book/111053 (дата обращения: 12.11.2020). - ISBN 978-5-9912-0470-5.

Нормативная литература

1. Методика определения актуальных угроз безопасности персональных данных при их обработке и информационных системах персональных данных (утв. 14 февраля 2008 г.) // ФСТЭК России [сайт]. – URL: https://fstec.ru/component/attachments/download/290 (дата обращения: 21.12.2024).
2. Р 1323565.1.035–2021. Информационная технология. Криптографическая защита информации. Использование российских криптографических алгоритмов в протоколе защиты информации ESP. Введен 01.06.2020. − М.: ИПК Издательство стандартов, 2001 − 36 с. – URL: https://docs.cntd.ru/document/603366557
3. Р 1323565.1.020-2020. Информационная технология. Криптографическая защита информации. Использование российских криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.2) радиочастот и внеполосные излучения радиопередатчиков гражданского применения. Введены 01.02 2019 г. − М.: 2020 − URL: https://docs.cntd.ru/document/603366546 (дата обращения 21.12.2024).
4. Р 1323565.1.030-2020. Информационная технология. Криптографическая защита информации. Использование криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.3). Введены 01.06.2020. − М.: 2020 − URL: https://docs.cntd.ru/document/573338314 (дата обращения 21.12.2024).

Периодические издания

1. Вопросы Кибербезопасности : научный журнал / Научно-производственное объединение Эшелон. - Москва : НПО Эшелон, 2013 - . - URL: https://cyberrus.info/ (дата обращения: 05.07.2025). - Режим доступа: свободный. - ISSN 2311-3456 /.
2. Information Security Информационная безопасность: журнал сайт. – URL: https://lib.itsec.ru/articles2/allpubliks (дата обращения 21.12.2024). - 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: 21.12.2024). - Режим доступа: свободный.
2. eLIBRARY.RU: Научная электронная библиотека: сайт. - Москва, 2000 -. - URL: https://www.elibrary.ru/defaultx.asp (дата обращения: 21.12.2024). - Режим доступа: для зарегистрированных пользователей.
3. IEEE/IET Electronic Library (IEL) [Электронный ресурс] = IEEE Xplore: Электронная библиотека. - USA; UK, 1998-. - URL: https://ieeexplore.ieee.org/Xplore/home.jsp (дата обращения: 21.12.2024). - Режим доступа: из локальной сети НИУ МИЭТ в рамках проекта "Национальная подписка"
4. Международный союз электросвязи: специализированное учреждение ООН: сайт. – URL: https://www.itu.int/ru/Pages/default.aspx (дата обращения: 21.12.2024). - Режим доступа: свободный.
5. 3GPP: Партнерский проект 3-го поколения: сайт. – URL: https://www.3gpp.org/ (дата обращения: 21.12.2024). - 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 21.12.2020)

- Сайт NIST. Раздел по безопасности Лаборатории информационных технологий Национального института по стандартизации США: сайт. – URL: https://www.nist.gov/cybersecurity (дата обращения 21.12.2020)

- 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 21.12.2020)

- Сайт ISACA. Information Systems Audit and Control Association (ISACA) Ассоциация по аудиту и управлению информационными системами: сайт. – URL: https://www.isaca.org/ (дата обращения 21.12.2020)

- Сайт TCG. Консорциум Trusted Computing Group (TCG) Группа по доверенным вычислениям: сайт. – URL: https://trustedcomputinggroup.org/ (дата обращения 21.12.2020)

- Сайт IEEE. Технический комитет IEEE по безопасности и приватности: сайт. – URL: http://www.ieee-security.org/ (дата обращения 21.12.2020)

- Сайт NIST. База данных уязвимостей продуктов информационной технологии Национального института по стандартизации США: сайт. – URL: https://nvd.nist.gov/vuln (дата обращения 21.12.2020)

- Сайт компании Offensive Security. База данных уязвимостей продуктов информационной технологии: сайт. – URL: https://www.exploit-db.com/ (дата обращения 21.12.2020)

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	Моноблоки 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	Моноблоки Dell Inspirion 3227(Intel Core i3-713U) с беспроводной клавиатурой и мышью	LibreOffice. Интернет браузер. Sumatra pdf. WireShark. Kleopatra. Code::Blocks.

Наименование учебных аудиторий и помещений для самостоятельной работы	Оснащенность учебных аудиторий и помещений для самостоятельной работы	Перечень программного обеспечения
		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 P lus или Open Office, браузер (Firefox, Google Crome); Acrobat reader DC

10. ФОНДЫ ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕРКИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ/ПОДКОМПЕТЕНЦИЙ

1. ФОС по подкомпетенции **ПК-4.БСС** «Способен обеспечивать информационную безопасность инфокоммуникационных систем».
2. ФОС по подкомпетенции **ПК-5.БСС** «Способен организовывать и проводить оценку работоспособности и эффективность применения программно-аппаратных средств защиты информации».

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

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.

Выполнение задания:

1) определение области знаний;

2) выбор типа и источников данных;

3) сбор материалов, необходимых для наполнения информационной модели;

4) отбор наиболее полезной информации;

5) выбор метода обработки информации (классификация, кластеризация, регрессионный анализ и т.д.);

6) выбор алгоритма поиска закономерностей;

7) поиск закономерностей, формальных правил и структурных связей в собранной информации;

8) творческая интерпретация полученных результатов;

9) ответы на контрольные вопросы, представленные в рекомендованной литературе.

Профессионально-ориентированное задание требует от студента умения анализировать в короткие сроки большой объем неупорядоченной информации, принятие решений в условиях недостаточной информации. Задание формулируется на основе практических проблемных ситуаций — кейсов, связанных с конкретными профессиональными действиями.

Выполнение задания:

1) подготовить основной текст с вопросами для обсуждения:

— титульный лист с названием задания;

— введение, где упоминается профессиональная задача, рассказывается об истории вопроса, указывается время начала действия;

— основная часть, где содержится главный массив информации, проблема;

— заключение (в нем решение проблемы, рассматриваемой в кейсе, иногда может быть не завершено);

2) подобрать приложения с подборкой различной информации, передающей общий контекст кейса (документы, публикации и др.);

3) предложить возможное решение проблемы.

4) рассмотреть достоинства и недостатки предложенного решения

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 индивидуального проекта 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 индивидуального проекта	до 14 недели
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 индивидуальных проектов;
- 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 (максимум 100 баллов), контрольные мероприятия в семестре (70 баллов) и экзамен (30 баллов).

В течении семестра основные контрольные мероприятия осуществляются на практических занятиях (всего 4 практических занятия). За контрольное мероприятие в рамках практического занятия учащийся может получить от 0 до 6 баллов. Контрольным мероприятием в течение 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., доцент _____/А.С. Волков/

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 29.08.2025 года, протокол № 1

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 /