

Смоленский колледж телекоммуникаций (филиал)
Федерального государственного бюджетного образовательного
учреждения высшего образования
«Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича»

УТВЕРЖДАЮ

Зам. директора по учебной работе

 И.А. Овчинникова

« 14 » 05 2025 г.

**РАБОЧАЯ ПРОГРАММА
ДИСЦИПЛИНЫ ОБЩЕПРОФЕССИОНАЛЬНОГО ЦИКЛА
ОП.13 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

среднего профессионального образования

для специальности

11.02.18 Системы радиосвязи, мобильной связи и телерадиовещания

г. Смоленск, 2025

РАССМОТРЕНО

на заседании методической комиссии
дисциплин сетей связи

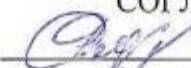
Председатель  Кожекина Е.Н.
Протокол № 11 «14» 05 2025 г.

СОГЛАСОВАНО

Начальник отдела защиты информации
Министерства цифрового развития
Смоленской области

 А.Н. Калугин
«14» 05 2025 г.

СОГЛАСОВАНО

Методист  Ряска О.Г.
«14» 05 2025 г.

Составитель: Грубник Е.М. – преподаватель СКТ (ф) СПбГУТ.

Рабочая программа разработана на основе ФГОС среднего профессионального образования по специальности 11.02.18 Системы радиосвязи, мобильной связи и телерадиовещания, утвержденного приказом Министерства просвещения РФ от 11 ноября 2022 г. № 963 (ред. от 03.07.2024).

СОДЕРЖАНИЕ

Название разделов	Страницы
1. Общая характеристика рабочей программы дисциплины ОП.13 Основы информационной безопасности	4
2. Структура и содержание дисциплины	5
3. Условия реализации рабочей программы дисциплины	8
4. Контроль и оценка результатов освоения дисциплины	11
Приложение 1	

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ ОП.13 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1. Область применения программы

Рабочая программа дисциплины ОП.13 Основы информационной безопасности является частью образовательной программы (ОП) СКТ(ф)СПбГУТ в соответствии с ФГОС СПО по специальности 11.02.18 Системы радиосвязи, мобильной связи и телерадиовещания.

1.2. Место дисциплины в структуре образовательной программы

Дисциплина ОП.13 Основы информационной безопасности относится к общепрофессиональным дисциплинам профессионального цикла ОП.

1.3. Цели и задачи дисциплины. Требования к результатам освоения дисциплины

Содержание дисциплины ориентировано на подготовку студентов для освоения профессиональных модулей по специальности 11.02.18 Системы радиосвязи, мобильной связи и телерадиовещания базовой подготовки и овладению следующими профессиональными (ПК) и общими (ОК) компетенциями:

ПК 3.1. Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности.

ПК 3.2. Разрабатывать комплекс методов и средств защиты информации в системах радиосвязи, мобильной связи и телерадиовещания.

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 02. Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности.

В результате освоения дисциплины студент должен уметь и знать
в вариативной части:

У 1 – классифицировать угрозы информационной безопасности в инфокоммуникационных системах и сетях связи;

У 2 – определять оптимальные способы обеспечения информационной безопасности;

У 3 - выявлять недостатки систем защиты в системах и сетях связи с использованием специализированных программных продуктов;

У 4 – проводить выбор средств защиты в соответствии с выявленными угрозами;

У 5 - разрабатывать политику безопасности объекта;

З 1 – принципы построения систем радиосвязи, мобильной связи и телерадиовещания;

З 2 - международные стандарты информационной безопасности;

З 3 - акустические и виброакустические каналы утечки информации, особенности их возникновения, организации, выявления и закрытия;

З 4 - технические каналы утечки информации, реализуемые в отношении объектов информатизации и технических средств предприятий связи, способы их обнаружения и закрытия;

З 5 - классификацию угроз сетевой безопасности;

З 6 - методы и способы защиты информации, передаваемой по проводным и беспроводным направляющим системам;

З 7 - возможные способы несанкционированного доступа;

З 8 - законодательные и нормативные правовые акты в области информационной безопасности;

З 9 - правила проведения возможных проверок.

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1. Объем дисциплины ОП.13 Основы информационной безопасности и виды учебной работы

Вид учебной работы	Объем часов
	Очная форма обучения
Максимальная учебная нагрузка (всего)	72
Обязательная аудиторная учебная нагрузка (всего)	72
в том числе:	
лекции	52*
практические занятия	20
Промежуточная аттестация - 4 семестр комплексный дифференцированный зачет (с ОП.09 Информационные технологии) в виде тестирования	2*

*Промежуточная аттестация в 4 семестре проводится за счет часов лекционной нагрузки

2.2. Тематический план и содержание дисциплины ОП.13 Основы информационной безопасности

Наименование разделов и тем	Содержание учебного материала, практических занятий		Объем часов	Формируемые компетенции
Тема 1. Информационная безопасность в системе национальной безопасности Российской Федерации (8 ч.)	1.	Место и роль информационной безопасности в системе национальной безопасности Российской Федерации.	2	ПК 3.1. ПК 3.2. ОК 01. ОК 02
	2.	Основы государственной информационной политики. Концепция комплексного обеспечения информационной безопасности.	2	
	3.	Органы обеспечения информационной безопасности и защиты информации, их функции и задачи, нормативная деятельность. Законодательно-правовые акты в области защиты информации.	2	
	Практические занятия:		2	
	4.	Практическое занятие № 1. Использование справочно-правовых систем и официальных источников информации регуляторов информационной безопасности.	2	
Тема 2. Основные понятия информационной безопасности (14 ч.)	1.	Понятие об информации как объекте защиты. Основные свойства защищаемой информации. Виды и формы представления информации. Информационные ресурсы.	2	ПК 3.1. ПК 3.2. ОК 01. ОК 02
	2.	Классификация информационных ресурсов. Правовой режим информационных ресурсов.	2	
	3.	Источники угроз информационной безопасности. Системная классификация угроз безопасности информации.	2	
	4.	Основные направления и методы реализации угроз. Каналы и методы несанкционированного доступа к информации.	2	
	5.	Уязвимости. Анализ уязвимостей системы. Методы оценки уязвимости информации.	2	
	Практические занятия:		4	
	6.	Практическое занятие № 2. Анализ угроз информационной безопасности и каналов утечки информации.	2	
	7.	Практическое занятие № 3. Контроль информационных потоков и предотвращение правонарушений действий с информацией.	2	
Тема 3. Основы обеспечения информационной безопасности (12 ч.)	1.	Анализ существующих методик определения требований к защите информации.	2	ПК 3.1. ПК 3.2. ОК 01. ОК 02
	2.	Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации.	2	
	3.	Виды мер и основные принципы защиты информации. Основные механизмы защиты информации. Система защиты информации.	2	
	4.	Радиотехническая защита как составная часть информационной безопасности.	2	
	Практические занятия:		4	
	5.	Практическое занятие № 4. Основные средства и способы обеспечения информационной безопасности.	2	
	6.	Практическое занятие № 5. Определение активов организации (предприятия), подлежащих защите.	2	
Тема 4. Построение систем	1.	Определение и основные способы несанкционированного доступа. Методы защиты от несанкционированного доступа.	2	

Наименование разделов и тем	Содержание учебного материала, практических занятий		Объем часов	Формируемые компетенции
защиты от угрозы нарушения конфиденциальности (10 ч.)	2.	Организационные методы защиты от несанкционированного доступа.	2	ПК 3.1. ПК 3.2. ОК 01. ОК 02
	3.	Инженерно-техническая защита от несанкционированного доступа. Построение систем защиты от угрозы утечки по техническим каналам.	2	
	4.	Основные направления и цели использования криптографических методов защиты.	2	
	Практические занятия		2	
	5.	Практическое занятие № 6. Построение систем защиты от угрозы утечки по техническим каналам.	2	
Тема 5. Построение систем защиты от угрозы нарушения целостности информации и отказа доступа (8 ч.)	1.	Защита целостности информации при хранении и обработке.	2	ПК 3.1. ПК 3.2. ОК 01. ОК 02
	2.	Защита целостности информации при ее передаче по каналам связи.	2	
	3.	Построение систем защиты от угрозы отказа доступа к информации.	2	
	Практические занятия		2	
	4.	Практическое занятие № 7. Защита беспроводных соединений на базе программного комплекса защиты информации (ПКЗИ).	2	
Тема 6 Основы обеспечения безопасности мобильных сетей (8 ч.)	1.	Обзор уязвимостей мобильных сетей. Перехват вызовов с помощью перехватчиков IMSI (IMSI Catheters).	2	ПК 3.1. ПК 3.2. ОК 01. ОК 02
	2.	Архитектура безопасности мобильных сетей.	2	
	3.	Архитектура безопасности 5G IMT2020 и последующих поколений.	2	
	Практические занятия:		2	
	4.	Практическое занятие № 8. Защита трафика мобильных устройств (на примере ViPNet Connect).	2	
Тема 7 Инженерная защита и техническая охрана объектов мобильной связи (10 ч.)	1.	Средства контроля доступа. Замки. Средства сигнализации. Средства наблюдения.	2	ПК 3.1. ПК 3.2. ОК 01. ОК 02
	2.	Автоматизированные системы контроля доступа на объекте оператора мобильной связи.	1	
	3.	Система контроля и управления доступа помещений на объекте оператора мобильной связи.	1	
	4.	Организационно-распорядительная защита информации. Работа с кадрами и внутриобъектовый режим.	2	
	Практические занятия:		4	
	5.	Практическое занятие № 9. Выбор технических средств для физической защиты объектов сотовой подвижной связи.	2	
	6.	Практическое занятие № 10. Выбор оборудования пункта централизованного наблюдения.	2	
Комплексный дифференцированный зачет с ОП.09 Информационные технологии			2	
Всего:			72	

3. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ ОП.13 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

3.1. Требования к минимальному материально – техническому обеспечению.

Обучение по программе дисциплины ОП.13 Основы информационной безопасности осуществляется в лаборатории информационной безопасности телекоммуникационных систем.

Технические средства обучения (персональные компьютеры, оргтехника):

- автоматизированные рабочие места студентов – 10 шт. (рабочая станция с двумя мониторами Dell SE2416H 24”, клавиатурой и мышью, процессор Intel Pentium Dual Core G4620 3.7 GHz, оперативная память DDR4 16 Gb, жесткий диск 1 Tb, видеоадаптер GTX 1050 2 Gb);

- автоматизированное рабочее место преподавателя (рабочая станция с двумя мониторами Dell SE2416H 24”, клавиатурой и мышью, процессор Intel Pentium Dual Core G4620 3.7 GHz, оперативная память DDR4 16 Gb, жесткий диск 1 Tb, видеоадаптер GTX 1050 2 Gb).

Учебный сервер в колледже (аппаратное обеспечение: не менее 2-х сетевых плат, 2-х ядерный процессор с частотой не менее 3 ГГц, оперативная память объемом не менее 4 Гб; жесткий диск объемом не менее 1Тб; лицензионное или свободно распространяемое программное обеспечение).

Типовое активное оборудование: сетевые маршрутизаторы, сетевые коммутаторы, сетевые хранилища, шлюзы VPN, сетевые адаптеры и карты, сетевые контроллеры.

Специальное программное обеспечение:

1. Программный комплекс ViPNet Client 4U для защиты рабочих мест пользователей и мобильных устройств, разработчик ИнфоТеКС, <https://infotecs.ru/>.
2. ВМ Astra Linux SE – разработчик ГК «Астра» (ООО «РусБИТех-Астра»), <https://astralinux.ru/products>.
3. ViPNet CryptoFile 4 (демо-версия), разработчик ИнфоТеКС, <https://infotecs.ru/>.
4. ViPNet PKI Client (демо-версия), криптографическая защита файлов, разработчик ИнфоТеКС, <https://infotecs.ru/>.
5. Демоверсия Континент-АП для Linux (версия 4.1.0.478), Континент АП/ZTN, разработчик ООО «Код безопасности», <https://www.securitycode.ru/>.
6. Демоверсия Континент ZTN для iOS и iPadOS, разработчик ООО «Код безопасности», <https://www.securitycode.ru/>.
7. ViPNet Mobile Client Security, разработчик ИнфоТеКС, <https://infotecs.ru/>.
8. Приложение для конфиденциального общения корпоративных пользователей ViPNet CSS Connect (демо-версия), разработчик ИнфоТеКС, <https://infotecs.ru/>.
9. Стенд Континент 3 КС (АПКШ «Континент» 3 КС), разработчик ООО «Код безопасности», <https://www.securitycode.ru/>.
10. Генератор паролей ViPNet Password Generator, разработчик ИнфоТеКС, <https://infotecs.ru/>.

3.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет- ресурсов, дополнительной литературы.

Основные источники
для преподавателей:

ОИ1. Щеглов, А. Ю. Защита информации: основы теории: учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. - Москва: Издательство Юрайт, 2023. - 309 с. - (Высшее образование). - ISBN 978-5-534-04732-5. - URL : <https://urait.ru/bcode/511998>.

ОИ2. Медведовский, И.Д. Практическое применение международного стандарта безопасности информационных систем ISO 17799 [Электронный ресурс] / И.Д. Медведовский. – Электрон. текст. дан. – Режим доступа: www.dsec.ru/cd-courses/iso_17799_cd.php/, свободный.

Для студентов:

ОИ1. Щеглов, А. Ю. Защита информации: основы теории: учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. - Москва : Издательство Юрайт, 2023. - 309 с. - (Высшее образование). - ISBN 978-5-534-04732-5. - URL : <https://urait.ru/bcode/511998>.

ОИ2. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. - 3-е изд., перераб. и доп. - Москва : Издательство Юрайт, 2023. - 161 с. - (Высшее образование). - ISBN 978-5-534-07248-8. - URL : <https://urait.ru/bcode/512268>.

ОИ3. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. - 2-е изд., перераб. и доп. - Москва : Издательство Юрайт, 2023. - 107 с. - (Высшее образование). - ISBN 978-5-534-16388-9. - URL : <https://urait.ru/bcode/530927>.

ОИ4. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. - 3-е изд., перераб. и доп. - Москва : Издательство Юрайт, 2023. - 161 с. - (Профессиональное образование). - ISBN 978-5-534-13948-8. - URL : <https://urait.ru/bcode/518006>.

ОИ5. Сафиуллина Л.Х. Информационная безопасность. Практические аспекты: учебник для вузов / Л.Х. Сафиуллина, А.Р. Касимова, Я.С. Рябов, А.М. Садыков, В.А. Богомолов. - Санкт-Петербург : Интермедия, 2021. - 240 с. - ISBN 978-5-4383-0205-6. - URL: <https://ibooks.ru/bookshelf/374959/reading>. - Текст: электронный.

ОИ6. Сычев Ю.Н. Защита информации и информационная безопасность : учебное пособие. - (Среднее профессиональное образование) / Ю.Н. Сычев. - Москва : Инфра-М, 2021. - 201 с. - ISBN 978-5-16-109176-0. - URL: <https://ibooks.ru/bookshelf/373406/reading>. - Текст: электронный.

Дополнительные источники

Для преподавателей:

ДИ1. Скрипник, Д. А. Общие вопросы технической защиты информации: учебное пособие / Д. А. Скрипник. - 3-е изд. - Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. - 424 с. - ISBN 978-5-4497-0336-1. - Текст: электронный // Электронный ресурс цифровой образовательной среды СПО PROОбразование: [сайт]. - URL: <https://profspo.ru/books/89451>. - Режим доступа: для авторизир. пользователей.

Для студентов:

ДИ1. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. - Москва : Издательство Юрайт, 2023. - 325 с. - (Профессиональное образование). - ISBN 978-5-534-00843-2. - URL : <https://urait.ru/bcode/512861>.

ДИ2. Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. - 2-е изд., испр. - Москва : Издательство Юрайт, 2023. - 473 с. - (Высшее образование). - ISBN 978-5-534-12474-3. - URL : <https://urait.ru/bcode/511138>.

ДИ3. Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. - Москва : Издательство Юрайт, 2023. - 349 с. - (Высшее образование). - ISBN 978-5-534-02883-6. - URL : <https://urait.ru/bcode/511890>.

ДИ4. Родичев Ю.А. Информационная безопасность. Национальные стандарты Российской Федерации. Учебное пособие. 3-е изд. - (Серия «Учебник для вузов»). - Санкт-Петербург : Питер, 2023. - 384 с. - ISBN 978-5-4461-2112-0. - URL: <https://ibooks.ru/bookshelf/390206/reading>. - Текст: электронный.

ДИ5. Родичев Ю, А. Информационная безопасность: нормативно-правовые аспекты: Учебное пособие. / Ю.А. Родичев. - Санкт-Петербург : Питер, 2021. - 272 с. - ISBN 978-5-4461-9992-1. - URL: <https://ibooks.ru/bookshelf/377372/reading>. - Текст: электронный.

ДИ6. Нефедов, В. И. Теория электросвязи : учебник для среднего профессионального образования / В. И. Нефедов, А. С. Сигов ; под редакцией В. И. Нефедова. - Москва : Издательство Юрайт, 2023. - 495 с. - (Профессиональное образование). - ISBN 978-5-534-01470-9. - Текст : электронный // Образовательная платформа Юрайт [сайт]. - URL: <https://urait.ru/bcode/512076>.

ДИ7. Братко, А. И. Автоматизированные системы управления и связь: основы электросвязи : учебное пособие / А.И. Братко. - Москва : ИНФРА-М, 2022. - 329 с. - (Среднее профессиональное образование). - DOI 10.12737/1013017. - ISBN 978-5-16-014957-8. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1854230>. – Режим доступа: по подписке.

ДИ8. Божедаров, Д. А. Основы телерадиовещания : учебное пособие / Д. А. Божедаров. - Саранск: МГУ им. Н.П. Огарева, 2020. - 148 с. - ISBN 978-5-7103-3965-7. - Текст : электронный // Лань: электронно-библиотечная система. - URL: <https://e.lanbook.com/book/204521>. - Режим доступа: для авториз. пользователей.

ДИ9. Кирпичникова, М. Ю. Системы видеонаблюдения и контроля доступа : учебно-методическое пособие / М. Ю. Кирпичникова. - Самара : ПГУТИ, 2021. - 109 с. - Текст : электронный // Лань : электронно-библиотечная система. - URL: <https://e.lanbook.com/book/301112>. - Режим доступа: для авториз. пользователей.

ДИ10. Поликанин, А. Н. Технические средства охраны и видеонаблюдения. Системы видеонаблюдения и тепловизионного контроля : учебное пособие / А. Н. Поликанин. - Новосибирск: СГУГиТ, 2021. - 46 с. - ISBN 978-5-907320-92-5. - Текст : электронный // Лань : электронно-библиотечная система. - URL: <https://e.lanbook.com/book/222380>. - Режим доступа: для авториз. пользователей.

Электронные ресурсы

1. Источники отечественных и зарубежных нормативных документов:

1.1. <http://www.etsi.org/>

1.2. <http://www.itu.int/>

1.3. <http://www.allcomponents.ru/>

2. Специализированные сайты для поиска документации по электронным компонентам (datasheet):

2.1. <http://www.okdatasheet.com/>

2.2. <http://www.allcomponents.ru/>

3. Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации [Электронный ресурс]: официальный сайт. - Режим доступа: <http://https://digital.gov.ru/ru/>, свободный.

4. Сайт Федеральной службы безопасности России (ФСБ России) [Электронный ресурс]. - Режим доступа: <http://www.fsb.ru>, свободный.

5. Сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России) [Электронный ресурс]. - Режим доступа: <http://www.fstec.ru/>, свободный.

6. Сайт проекта Общие критерии оценки безопасности информационных технологий [Электронный ресурс]. - Режим доступа: <http://www.commoncriteriaportal.org/>, свободный.

7. Comnews. Новости телекоммуникаций, вещания и ИТ [Электронный ресурс]: ежедневная Интернет-газета. - Режим доступа: <http://www.comnews.ru/>, свободный.

8. Mobile Review [Электронный ресурс]: портал мобильных технологий. - Режим доступа: <http://www.mobile-review.com/>, свободный.

9. Открытые системы [Электронный ресурс]. - Режим доступа: <http://www.osp.ru/>, свободный.

10. Сети и системы связи [Электронный ресурс]: архив журнала. - Режим доступа: <http://www.ccc.ru/>, свободный.

11. Системы управления, связи и безопасности [Электронный ресурс]: сетевой электронный журнал. - Режим доступа: <http://sccs.intelgr.com/>, свободный.

12. Современные телекоммуникации России [Электронный ресурс]: отраслевой информационно-аналитический онлайн-журнал. - Режим доступа: <http://www.telecomru.ru/>, свободный.

13. Электронная Россия [Электронный ресурс]: информационный сайт. - Режим доступа: <http://www.elrussia.ru/>, свободный.

14. Электросвязь [Электронный ресурс]: сайт журнала. - Режим доступа: <http://www.elsv.ru/>, свободный.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения дисциплины ОП.13 Основы информационной безопасности осуществляются преподавателем в процессе проведения практических занятий, тестирования.

Код и наименование ПК и ОК, формируемых в рамках освоения общепрофессиональной дисциплины	Критерии оценки	Методы оценки
ПК 3.1. Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности.	- четкое понимание проблем информационной безопасности в системах радиосвязи, мобильной связи и телерадиовещания; - грамотное выявление, классификация и анализ угроз информационной безопасности и формы их проявления; - умение определять оптимальные способы обеспечения информационной безопасности; - знание принципов построения систем радиосвязи, мобильной связи и телерадиовещания; - знание международных стандартов информационной безопасности; - знание акустических и виброакустических каналов утечки информации, особенностей их возникновения, организации, выявления и закрытия; - знание технических каналов утечки информации, реализуемых в отношении объектов информатизации и технических средств предприятий связи, способов их обнаружения и закрытия.	- выполнение практических заданий, - результаты тестирования.
ПК 3.2. Разрабатывать комплекс методов и средств защиты информации в системах радиосвязи, мобильной связи и телерадиовещания.	- умение выявлять недостатки систем защиты в системах и сетях связи с использованием специализированных программных продуктов; - знание методов и способов защиты информации, передаваемой по проводным и беспроводным направляющим системам; - полнота владения сервисами, обеспечивающими информационную безопасность в системах радиосвязи, мобильной связи и телерадиовещания;	- выполнение практических заданий, - результаты тестирования.
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	- умение распознавать задачу и/или проблему в профессиональном и/или социальном контексте; - анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; составлять план действия; - определять необходимые ресурсы; - владение актуальными методами работы в профессиональной и смежных сферах; реализовывать составленный план; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника);	- выполнение практических заданий, - результаты тестирования.
ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	- быстрое определение сути задачи для поиска информации; - необходимых источников информации; планирование процесса поиска; структурирование получаемой информации; - оценивание практической значимости результатов поиска; - применение средств информационных технологий для решения профессиональных задач; использование современного программного обеспечения; различных цифровых средств для решения профессиональных задач.	- выполнение практических заданий, - результаты тестирования.

Лист изменений рабочей программы

Содержание изменения, страница рабочей программы	Дата и номер протокола заседания МК	Основание изменения
1.		
2.		
3.		