МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ
И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
Северо-Кавказский филиал
ордена Трудового Красного Знамени федерального государственного
бюджетного образовательного учреждения высшего образования
«Московский технический университет связи и информатики»

Утверждаю
Зам. директора по УВР
_____ Н.А. Андреева
«29» 04 2024 г.

# Программно-аппаратные средства защиты информации Б1.О.30

рабочая программа дисциплины

Кафедра: **Информационной безопасности**
Направление подготовки: **10.03.01 Информационная безопасность**
Профиль: **Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)**
Формы обучения: **очная**

**Распределение часов дисциплины по семестрам (для очной формы обучения (ОФО))**

| Вид учебной работы | ОФО | |
|---|---|---|
| | ЗЕ | часов |
| Общая трудоемкость дисциплины, в том числе (по семестрам, курсам): | 4 | 144/6 сем |
| Контактная работа, в том числе (по семестрам, курсам): | | 52/6 сем |
| Лекции | | 18/6 сем |
| Лабораторных работ | | 18/6 сем |
| Практических занятий | | 16/6 сем |
| Семинаров | | |
| Самостоятельная работа | | 56/6 сем |
| Контроль | | 36/6 сем |
| Число контрольных работ (по курсам) | | |
| Число КР (по семестрам, курсам) | | |
| Число КП (по семестрам, курсам) | | |
| Число зачетов с оценкой с разбивкой по семестрам (курсам) | | |
| Число экзаменов с разбивкой по семестрам (курсам) | | 1/6 сем |

Программу составил:
***Доцент кафедры ИТСС, к.т.н., доцент Решетникова И.В.***

Рецензенты:
***Ведущий сотрудник ФГУП «РНИИРС», д.т.н., доцент Елисеев А.В.***

Рабочая программа дисциплины
**«Программно-аппаратные средства защиты информации»**

разработана в соответствии с ФГОС ВО:
**направления подготовки 10.03.01 «Информационная безопасность», утвержденным приказом Министерства образования и науки Российской Федерации от 17 ноября 2020 г. N 1427.**

Составлена на основании учебного плана
**направления 10.03.01 «Информационная безопасность», профиля «Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)», одобренного Учёным советом СКФ МТУСИ, протокол № 9 от 22.04.2024, и утвержденного директором СКФ МТУСИ 22.04.2024 г.**

Рассмотрена и одобрена на заседании кафедры
«Информационная безопасность»

Протокол от «24» апреля 2024 г. № 9

Зав. кафедрой _____ Д.В. Маршаков

**Визирование для использования в 20__/20__ уч. году**

Утверждаю
Зам. директора по УВР _____
-__ _____ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры
"Информационная безопасность"

Протокол от _ _____ 20__ г. № _
Зав. кафедрой _____

---

**Визирование для использования в 20__/20__ уч. году**

Утверждаю
Зам. директора по УВР _____
-__ _____ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры

"Информационная безопасность"

Протокол от _ _____ 20__ г. № _
Зав. кафедрой _____

---

**Визирование для использования в 20__/20__ уч. году**

Утверждаю
Зам. директора по УВР _____
-__ _____ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры
"Информационная безопасность"

Протокол от _ _____ 20__ г. № _
Зав. кафедрой _____

---

**1. Цели изучения дисциплины**

Целями изучения дисциплины ***"Программно-аппаратные средства защиты информации"*** являются формирование у обучаемых знаний в области методов и средств инженерной защиты информации, а также возможностями их использования в реальных задачах создания и внедрения инфокоммуникационных систем.

**2. Планируемые результаты обучения**

Изучение дисциплины направлено на формирование у выпускника способности решать профессиональные задачи в соответствии с ***эксплуатационной деятельностью.***

Результатом освоения дисциплины являются сформированные у выпускника следующие компетенции:

| **Компетенции выпускника, формируемые в результате освоения дисциплины (в части, обеспечиваемой дисциплиной)** |
|---|
| **ОПК-8: способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности** |
| **Знать:** |
| - нормативные и методические материалы по вопросам оценки уровня защищенности объекта защиты информации;<br>- перечень необходимых вопросов по выбору справочной литературы по вопросам обеспечения информационной безопасности . |
| **Уметь:** |
| - осуществлять подбор нормативных и методических материалов по вопросам применения средств защиты информации;<br>- осуществлять изучение и обобщение научно-технической литературы, составлять обзор по вопросам обеспечения информационной безопасности |
| **Владеть:** |
| - навыками работы с нормативными и методическими материалами по вопросам применения средств защиты информации;<br>- навыками работы со справочной и научно-технической литературой по вопросам обеспечения информационной безопасности |
| **ОПК-10: способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты** |
| **Знать:** |
| программно-аппаратные средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях |
| **Уметь:** |
| конфигурировать программно-аппаратные средства защиты информации в соот-ветствии с заданными политиками безопасности |
| **Владеть:** |
| навыками реализации комплекса мер по обеспечению информационной безопасности |

**3. Место дисциплины в структуре образовательной программы**

| **Требования к предварительной подготовке обучающегося (предшествующие дисциплины, модули, темы):** | |
|---|---|
| 1 | Б1.О.27 Основы информационной безопасности |
| 2 | Б1.О.06 Высшая математика |
| **Последующие дисциплины и практики, для которых освоение данной** | |

| дисциплины необходимо: | |
|---|---|
| 1 | Б1.О.36.02 Криптографические протоколы |
| 2 | Б1.В.02 Стеганографические методы скрытия информации |
| 4 | Б1.О.33 Комплексное обеспечение защиты информации объекта информатизации |

Рабочая программа дисциплины для инвалидов и лиц с ограниченными возможностями здоровья разрабатывается индивидуально с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

**4. Структура и содержание дисциплины**

**4.1 Очная форма обучения, 4 года (всего 144 часов, 52 аудиторных часов, 56 часов самостоятельной работы)**

| Код зан. | Тема и краткое содержание занятия | Вид зан. | Кол. часов | Компетенции | УМИО |
|---|---|---|---|---|---|
| **Курс 3, Семестр 6** | | | | | |
| **Модуль 1. Концепция инженерно-технической защиты информации.** | | | | | |
| 1.1 | Лекция 1. Основные определения и понятия.<br>1. Характеристика инженерно-технической за-щиты информации как области информационной безопасности.<br>2. Основные проблемы инженерно-технической защиты информации.<br>3. Представление сил и средств защиты информации в виде системы.<br>4. Основные параметры системы защиты информации | Л1. | 2 | ОПК-8 | Л1.1<br>Л1.2<br>Л2.1<br>Л2.2 |
| 1.2 | Лекция 2. Теоретические основы инженерно-технической защиты информации. Особенности информации как предмета защиты.<br>1. Цели и задачи защиты информации. Ресурсы, выделяемы на защиту информации.<br>2. Принципы защиты информации техни-ческими средствами.<br>3. Основные направления инженерно-технической защиты информации. Показатели эффективности инженерно-технической защиты информации. | Л2. | 4 | ОПК-8 | Л1.1<br>Л1.2<br>Л2.1<br>Л2.2 |
| 1.3 | Лекция 3. Характеристика технической разведки Основные задачи и органы технической разведки.<br>Демаскирующие признаки радиоэлектронных средств<br>Виброакустические технические каналы утечки речевой информации | Л3. | 4 | ОПК-8 | Л1.1<br>Л1.2<br>Л2.1<br>Л2.2 |
| 1.4 | Практическая работа 1.<br>Изучение законодательной и нормативной базы правового регулирования вопросов защиты информации | ПЗ1. | 2 | ОПК-8 | Л3.1 |
| 1.5 | Практическая работа 2.<br>Изучение задач и функций органов по технической защите информации в РФ | ПЗ2 | 2 | ОПК-8 | Л3.1 |
| 1.6 | Практическая работа 3.<br>Изучение положений о государственном лицензировании деятельности в области защиты информации | ПЗ3 | 4 | ОПК-8 | Л3.1 |
| 1.7 | Лабораторная работа №1.<br>Организация аттестации выделенного помещения по требованиям безопасности информации | ЛР 1 | 4 | ОПК-8 | Л3.1 |

| | | | | | |
|---|---|---|---|---|---|
| 1.8 | Лабораторная работа №2.<br>Статистический анализ загрузки заданного радиодиапазона и обнаружение радиозакладных устройств в защищаемом помещении | ЛР 2 | 4 | ОПК-8 | Л3.1 |
| 1.9 | Демаскирующие признаки объектов Параметрические технические каналы утечки речевой информации<br>Акустоэлектрические каналы утечки речевой информации<br>Демаскирующие признаки объектов в видимом диапазоне<br>Демаскирующие признаки объектов в инфракрасном диапазоне | СРС | 36 | ОПК-8 | Л1.1<br>Л1.2<br>Л2.1<br>Л2.2 |
| **Модуль 2 Технический контроль эффективности мер защиты информации** | | | | | |
| 2.1 | Лекция 4. . Общие вопросы организации противодействия технической разведке.<br>1. Основные организационные и технические мероприятия, используемые для противодействия технической разведке.<br>2. Методы и средства защиты режимных объек-тов от утечки конфиденциальной информации по техническим каналам.<br>3. Физические основы образования побочных электромагнитных излучений от технических средств. | Л4 | 4 | ОПК-10 | Л1.1<br>Л1.2<br>Л2.1<br>Л2.2 |
| 2.2 | Лекция 5. Идентификация пользователей и установление их подлинности при доступе к компьютерным ресурсам.<br>1. Основные этапы доступа к ресурсам вычислительной системы.<br>2. Использование простого пароля; использование динамически изменяющегося пароля; взаимная проверка подлинности и другие случаи опознания.<br>3. Способы разграничения доступа к компьютерным ресурсам; разграничение доступа по спискам. | Л5 | 2 | ОПК-10 | Л1.1<br>Л1.2<br>Л2.1<br>Л2.2 |
| 2.3 | Лекция 6. Цели и задачи технического контроля эффективности мер защиты информации<br>1. Порядок проведения контроля защищенности информации на объекте ВТ от утечки по каналу ПЭМИ<br>2. Порядок проведения контроля защищенности АС от НСД<br>3. Методы контроля побочных электромагнит-ных излучений генераторов технических средств | Л5 | 2 | ОПК-10 | Л1.1<br>Л1.2<br>Л2.1<br>Л2.2 |
| 2.4 | Практическое занятие №4<br>Изучение положений о сертификации средств защиты информации по требованиям безопасности информации | ПЗ4 | 4 | ОПК-10 | Л3.1 |
| 2.5 | Практическое занятие № 5<br>Изучение положения о сертификации средств вычислительной техники и связи | ПЗ5 | 2 | ОПК-10 | Л3.1 |
| 2.6 | Практическое занятие № 6<br>Изучение типовой методики испытаний объектов информатики по требованиям безопасности информации | ПЗ6 | 2 | ОПК-10 | Л3.1 |
| 2.7 | Лабораторная работа № 3<br>«Исследование детектора электромагнитного поля ST107». | ЛРЗ | 4 | ОПК-10 | Л3.1 |

| | | | | | |
|---|---|---|---|---|---|
| 2.8 | Лабораторная работа № 4<br>Обнаружение сигналов линейных и сетевых закладок | ЛР4 | 6 | ОПК-10 | Л3.1 |
| 2.9 | Способы предотвращения утечки информации через ПЭМИН ПК<br>Методы средства ограничения доступа к компонентам ЭВМ<br>Надёжность средств защиты компонент; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям<br>Безопасность оптоволоконных кабельных систем.<br>Заземление технических средств и подавление информационных сигналов в цепях заземления | СРС | 20 | ОПК-10 | Л1.1<br>Л1.2<br>Л2.1<br>Л2.2 |
| | **Экзамен** | | 36 | | |
| **Итого – 144 часа** | | | | | |

## 5. Учебно-методическое и информационное обеспечение дисциплины

**5.1. Рекомендуемая литература**

**5.1.1. Основная литература**

| Код | Авторы, составители | Заглавие | Издательство, год | Кол. |
|---|---|---|---|---|
| Л1.1 | Зайцев, А. П. | Технические средства и методы защиты информации: Учебник для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В.Мещеряков; Под ред. А.П.Зайцева - 7 изд., исправ. - | Москва : Гор. линия-Телеком, 2012. - 442с.; - (Уч. для вузов). ISBN 978-5-9912-0233-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/390284 . – Режим доступа: по подписке. | Э1 |
| Л1.2 | Душкин А.В., Барсуков О.М., Кравцов Е.В. | Программно-аппаратные средства обеспечения информационной безопасности: | Учебное пособие для вузов / Душкин А.В., Барсуков О.М., Кравцов Е.В. - Москва :Гор. линия-Телеком, 2016. - 248 с. (Специальность) ISBN 978-5-9912-0470-5. - Текст : электронный. - URL: https://znanium.com/catalog/product/973806 . – Режим доступа: по подписке. | Э2 |

**5.1.2. Дополнительная литература**

| Код | Авторы, составители | Заглавие | Издательство, год | Кол. |
|---|---|---|---|---|
| Л2.1 | Новиков, С.Н. | Методология защиты пользовательской информации на основе технологий сетевого уровня мультисервисных сетей связи / С.Н. Новиков ; под ред. В.П. Шува- | Москва : Горячая линия -Телеком, 2018. - 128 с. - ISBN 978-5-9912-0410-1. - Текст : | Э3 |

| | | | | |
|---|---|---|---|---|
| | | лова. -- | электронный. - URL: https://znanium.com/catalog/product/1040260 – Режим доступа: по подписке.. | |
| Л2.2 | Новиков, В. К. | Организационно-правовые основы информационной безопасности (защиты информации). Юридическая ответственность за правонарушения в области ...: | Уч. пос./НовиковВ.К. - Москва : Гор. линия-Телеком, 2015.- 176с. (О)ISBN 978-5-9912-0525-2, 500 экз. - Текст : электронный. - URL: https://znanium.com/catalog/product/536932 . – Режим доступа: по подписке. | Э4 |

**5.1.3. Учебно-методическое обеспечение для самостоятельной работы обучающихся**

| Код | Авторы, составители | Заглавие | Издательство, год | Кол. |
|---|---|---|---|---|
| Л3.1 | Решетникова И.В | ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ-ИСЕТЕЙ И СИСТЕМ. Учебное пособие. – Ростов-на-Дону: СКФ МТУСИ, 2022. – 52 с. | РнД: СКФ МТУСИ, 2022 | Э5 |

**5.2. Электронные образовательные ресурсы**

| | |
|---|---|
| Э1 | https://znanium.com/catalog/document?pid=390284 |
| Э2 | https://znanium.com/catalog/document?id=329375 |
| Э3 | https://znanium.com/catalog/document?id=343949 |
| Э4 | https://znanium.com/catalog/document?id=67242 |
| Э5 | http://www.skf-mtusi.ru/?page_id=659 |

**5.3. Программное обеспечение**

| | |
|---|---|
| П.1 | Linux (свободное ПО) |
| П.2 | LibreOffice (свободное ПО) |
| П.3 | Kaspersky Endpoint Security (лицензия) |

## 6. Материально-техническое обеспечение дисциплины

| | |
|---|---|
| 6.1 МТО лекционных занятий | |
| 1 | Лекционная аудитория, оборудованная интерактивной доской, проектором |
| 6.2 МТО лабораторных работ и практических занятий | |
| 1 | Компьютерные аудитории с возможностью выхода в локальную сеть Филиала и Интернет |
| 6.3 МТО рубежных контролей, экзамена | |
| 1 | Компьютерные аудитории с возможностью выхода в локальную сеть Филиала и Интернет |

## 7. Методические рекомендации для обучающихся по самостоятельной работе

### Указания по подготовке к различным видам занятий

Подготовка к лекционным занятиям осуществляется систематически и сводится к повторению изученного материала и отработке тем, вынесенных на самостоятельную работу. При этом должен быть доработан конспект лекций, а также получены ответы на контрольные вопросы, которые, как правило, приводятся в конце каждого раздела учебных пособий. Особое внимание необходимо уделить пониманию изучаемого материала. Зафиксировать вопросы, которые следует задать преподавателю.

Подготовка к лабораторным и практическим занятиям должна проводиться в объеме тех указаний, которые приводятся в каждом методическом пособии для проведения соответствующего занятия. Тема очередного занятия объявляется преподавателем накануне.

После повторения лекционного материала необходимо ознакомиться с предлагаемыми практическими заданиями, уяснить их суть, продумать порядок их выполнения, уточнить достаточность своих знаний для выполнения задания. Целесообразно выполнить возможные заготовки из состава отчета, который предстоит оформить на занятии. Это позволит выполнить и защитить работу в период плановых часов. Перед проведением каждого занятия должно быть полное представление о сути и порядке выполнения предстоящей работы.

Существенное значение имеет самостоятельная работа студента.

Темы для самостоятельного изучения для различных форм обучения, информационные источники и рекомендуемое время указаны в Разделе 4 настоящей Рабочей программы.

Самостоятельная работа студентов по дисциплине проводится в течение всего семестра и складывается из нескольких составляющих.

**Подготовка к плановым аудиторным занятиям.** В начале семестра студентов знакомят с календарным планом проведения всех видов учебных занятий. Чтобы студенты могли проверить качество своей подготовки к занятиям, в учебных пособиях и методических указаниях к лабораторным работам имеются вопросы для проверки уровня знаний перед выполнением работы и контрольные вопросы, позволяющие студенту оценить качество полученных результатов после выполнения работы. Предлагаемые студентам учебные пособия кроме контрольных вопросов содержат примеры с решениями и упражнения по основным темам.

**Изучение технической литературы.** Студенты самостоятельно изучают рекомендованную преподавателем техническую литературу.

**Дополнительные самостоятельные исследования в лаборатории**. Студенты, желающие получить более глубокие знания, имеют возможность выполнить дополнительные самостоятельные исследования в лаборатории. С этой целью в плановых лабораторных работах предусмотрены возможности для дополнительных исследований. Перечень разделов программы, предлагаемых для самостоятельных исследований, доводится до сведения студентов в начале семестра.

**Самостоятельная работа на ПЭВМ**. Для повышения эффективности самостоятельной работы студентам во второй половине дня предоставляется возможность выполнить в лаборатории самостоятельные исследования с использованием программно-аппаратного комплекса, состоящего из виртуальных электронных приборов, отображаемых на экране ПЭВМ, и моделирующих программ. Исследуемые схемы могут собираться из реальных компонентов на лабораторном стенде или виртуальных компонентов, хранящихся в библиотеке ПЭВМ.

### Источники, рекомендуемые для углубленного изучения учебного материала


1. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие. – М.: ДМК Пресс, 2011. – 416 с.;
2. Бирюков А.А. Информационная безопасность: защита и нападение. 2-е изд., перераб. и доп. – М.: ДМК Пресс, 2017. – 434 с.
3. Маршаков, Д. В. Программно-аппаратные средства защиты информации: учебное посо-

бие / Д. В. Маршаков, Д. В. Фатхи. — Ростов-на-Дону: Донской ГТУ, 2021. — 228 с.
4. Воронов В.А., Тихонов В.А. Концептуальные основы создания и применения системы защиты объектов. – М.: Горячая линия - Телеком, 2013.
5. Хорев П.Б. Программно-аппаратная защита информации: учебное пособие. 3-е изд., испр. и доп. – Москва: ИНФРА-М, 2022. – 327 с.
6. Ерохин С.Д., Петухов А.Н., Пилюгин П.Л. Управление безопасностью критических информационных инфраструктур. – М.: Горячая линия – Телеком, 2021.
7. Климентьев, К. Е. Введение в защиту компьютерной информации: учебное пособие / К. Е. Климентьев. — Самара: Самарский университет, 2020. — 183 с.
8. Краковский, Ю. М. Методы защиты информации: учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург: Лань, 2021. — 236 с..
9. Никифоров, С. Н. Методы защиты информации. Пароли, скрытие, шифрование: учеб-ное пособие для вузов / С. Н. Никифоров. — 4-е изд., стер. — Санкт-Петербург: Лань, 2022. — 124 с.
10. Язов Ю.К., Соловьев С.В. Организация защиты информации в информационных системах от несанкционированного доступа: монография / Ю.К. Язов, С.В. Соловьев. – Воронеж: Кварта, 2018. – 588 с.
11. Профильные журналы «Электросвязь», «T-Comm: Телекоммуникации и транспорт» и другие.

**Использование Интернет-ресурсов**

1. Электронный ресурс https://www.securitylab.ru/
2. Электронный ресурс https://securelist.ru/
3. Электронный ресурс https://www.kaspersky.ru/
4. Электронный ресурс https://encyclopedia.kaspersky.ru/
5. Электронный ресурс https://www.drweb.ru/
6. Электронный ресурс http://infoprotect.net/category/news
7. Электронный ресурс https://www.it-world.ru/it-news/security/
8. Электронный ресурс https://threatpost.ru/
9. Электронный ресурс https://www.anti-malware.ru/

**Рекомендации по подготовке к рубежным аттестациям**

Подготовка к сдаче модуля сводится защите на дату проведения последнего занятия в рамках модуля всех практических и лабораторных занятий, а также к подготовке к ответам по тестовым заданиям.

Объем вопросов по каждому лабораторному и практическому занятию отражен в методических указаниях по проведению соответствующего занятия. Кроме того студент должен быть готов к пояснениям по сути практических приемов работы и доказыванию обоснованности принятых решений. Если работа не выполнена или не защищена своевременно, то это следует сделать в часы самоподготовки и консультаций до даты последнего занятия в рамках сдаваемого модуля.

Подготовка к выполнению теста обеспечивается изучением и повторением того материала, который изучался на лекционных занятиях и входе лабораторных и практических занятий. Материал повторяется по конспектам и учебным пособиям, указанным в списке литературы и методических указаниях.

Подготовка к экзамену осуществляется на протяжении всего времени изучения дисциплины.

Для более конкретной, целенаправленной и качественной подготовки к экзамену необходимо перед началом изучения дисциплины познакомиться с содержанием рабочей программы. Уяснить логику и последовательность изучения материала, уточнить конкретные конечные результаты, которые должны быть достигнуты в итоге изучения конкретных тем и занятий. Познакомиться с перечнем вопросов и заданий, выносимых на экзамен.

В ходе каждого занятия необходимо изучить все учебные вопросы и выполнить практические задания. Для оперативного оценивания уровня достижения учебных целей следует ответить на кон-

трольные вопросы, которые имеются в руководстве для каждого практического и лабораторного занятия. В случае выявленных затруднений следует провести дополнительное изучение материала в часы самостоятельной работы или в период консультаций с преподавателем. Все учебные материалы должны быть отражены в конспекте, он должен дополняться и уточняться по мере отработки и уточнения учебных вопросов. Само ведение конспекта концентрирует внимание, упорядочивает знания, стимулирует активность в усвоении. К моменту выхода на непосредственную подготовку к зачету в конспекте не должно остаться непонятных вопросов.

В силу ограниченного времени, отводимого на непосредственную подготовку к экзамену, целесообразно материал повторять в основном по отработанному конспекту. Это экономит время и дает возможность работать по уже знакомым записям, что улучшает запоминание материала. Остается спланировать работу в соответствии с имеющимся временем и жестко придерживаться намеченного плана. В период обязательных плановых предэкзаменационных консультаций необходимо уточнить организационные вопросы проведения экзамена и при необходимости - сложные вопросы по существу материала.

**Дополнения и изменения в Рабочей программе**