МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»

УТВЕРЖДАЮ:

Директор ИУЦТ

С.П. Вакуленко

30 апреля 2020 г.

Кафедра «Вычислительные системы, сети и информационная безопасность»

Автор Сафонова Ирина Евгеньевна, д.т.н., доцент

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Методы оценки безопасности компьютерных систем

Направление подготовки:	10.03.01 – Информационная безопасность
Профиль:	Безопасность компьютерных систем
Квалификация выпускника:	Бакалавр
Форма обучения:	очная
Год начала подготовки	2020

Одобрено на заседании	Одобрено на заседании кафедры
Учебно-методической комиссии института Протокол № 4 30 апреля 2020 г. Председатель учебно-методической комиссии Н.А. Клычева	Протокол № 15 27 апреля 2020 г. Заведующий кафедрой Б.В. Желенков

Москва 2020 г.

1. ЦЕЛИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целями освоения учебной дисциплины «Методы оценки безопасности компьютерных систем» являются формирование компетенций по основным разделам данного курса, изучение студентами основных методов оценки безопасности компьютерных систем, стандартов в этой области; получение представления об организации и принципах обеспечения информационной безопасности компьютерных систем.
Студенты должны научиться применять современные методы оценки безопасности компьютерных систем.

Дисциплина формирует знания и умения для решения следующих профессиональных задач (в соответствии с видами профессиональной деятельности):

Эксплуатационной:
- установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований;
- администрирование подсистем информационной безопасности объекта;
- участие в проведении аттестации объектов информатизации по требованиям безопасности информации и аудите информационной безопасности автоматизированных систем;

Проектно-технологической:
- сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности;
- проведение проектных расчетов элементов систем обеспечения информационной безопасности;
- участие в разработке технологической и эксплуатационной документации;
проведение предварительного технико-экономического обоснования проектных расчетов;

Организационно-управленческой:
- осуществление организационно-правового обеспечения информационной безопасности объекта защиты;
- организация работы малых коллективов исполнителей;
- участие в совершенствовании системы управления информационной безопасностью;
- изучение и обобщение опыта работы других учреждений, организаций и предприятий в области защиты информации, в том числе информации ограниченного доступа;
- контроль эффективности реализации политики информационной безопасности объекта защиты.

Экспериментально-исследовательской:
- сбор, изучение научно-технической информации, отечественного и зарубежного опыта по тематике исследования;
- проведение экспериментов по заданной методике, обработка и анализ их результатов;
проведение вычислительных экспериментов с использованием стандартных программных средств.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Учебная дисциплина "Методы оценки безопасности компьютерных систем" относится к блоку 1 "Дисциплины (модули)" и входит в его вариативную часть.

2.1. Наименования предшествующих дисциплин

Для изучения данной дисциплины необходимы следующие знания, умения и навыки, формируемые предшествующими дисциплинами:

2.1.1. Криптографические методы защиты информации:

Знания: понятия, определения, термины (понятийный аппарат курса)признаки, параметры, характеристики, свойства изучаемых в курсе объектов; методы, средства, приемы, алгоритмы, способы решения задач курса

Умения: оформлять, представлять, описывать, характеризовать данные, сведения, факты, результаты работы на языке символов (терминов, формул, образов), введенных и используемых в курсе; рассчитывать, определять, находить, решать, вычислять, оценивать, измерять признаки, параметры, характеристики, величины, состояния, используя известные модели, методы, средства, решения, технологии, приемы, алгоритмы, законы, теории, закономерности; выбирать способы, методы, приемы, алгоритмы, меры, средства, модели, законы, критерии для решения задач курса изменять, дополнять, адаптировать, развивать методы, алгоритмы, средства, решения, приемы, методики для решения конкретных задач

Навыки: работать с компьютером как средством управления информацией

2.1.2. Основы информационной безопасности :

Знания: основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ России, ФСТЭК России в данной области; правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны

Умения: анализировать и оценивать угрозы информационной безопасности объекта; пользоваться нормативными документами по защите информации; разрабатывать концепции и политикинеобходимые для эффективного функционирования комплексных систем информационной безопасности объектов информатизации;

Навыки: профессиональной терминологией; навыками применения средств антивирусной защиты; навыками организации и обеспечения режима защиты информации; навыками использования технических средств защиты информации; методами и средствами выявления угроз и уязвимостей безопасности объектов информатизации.

2.1.3. Техническая защита информации:

Знания: эксплуатационные параметры и технические характеристики аппаратных и технических средств защиты информации.

Умения: проверять работоспособность элементов системы защиты с помощью необходимых технических средств

Навыки: основными приемами организации комплексной системы информационной безопасности, включая организационное, правовое и техническое обеспечение.

2.2. Наименование последующих дисциплин

Результаты освоения дисциплины используются при изучении последующих учебных дисциплин:

2.2.1. Комплексное обеспечение защиты объекта информатизации

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫЕ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

В результате освоения дисциплины студент должен:

№ п/п	Код и название компетенции	Ожидаемые результаты
1	ПКР-2 Способность участвовать в разработке политик безопасности, политик управления доступом и информационными потоками в компьютерных сетях.	ПКР-2.1 Знать виды политик управления доступом и информационными потоками в компьютерных сетях. ПКР-2.2 Уметь обосновывать выбор используемых программно-аппаратных средств защиты информации в компьютерных сетях. ПКР-2.3 Владеть навыками разработки порядка применения программно-аппаратных средств защиты информации в компьютерных сетях.

4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ) В ЗАЧЕТНЫХ ЕДИНИЦАХ И АКАДЕМИЧЕСКИХ ЧАСАХ

4.1. Общая трудоемкость дисциплины составляет:

3 зачетные единицы (108 ак. ч.).

4.2. Распределение объема учебной дисциплины на контактную работу с преподавателем и самостоятельную работу обучающихся

	Количество часов	
Вид учебной работы	Всего по учебному плану	Семестр 7
Контактная работа	54	54,15
Аудиторные занятия (всего):	54	54
В том числе:		
лекции (Л)	36	36
практические (ПЗ) и семинарские (С)	18	18
Самостоятельная работа (всего)	54	54
ОБЩАЯ трудоемкость дисциплины, часы:	108	108
ОБЩАЯ трудоемкость дисциплины, зач.ед.:	3.0	3.0
Текущий контроль успеваемости (количество и вид текущего контроля)	ПК1, ПК2	ПК1, ПК2
Виды промежуточной аттестации (экзамен, зачет)	ЗаО	ЗаО

4.3. Содержание дисциплины (модуля), структурированное по темам (разделам)

№ п/п	Семестр	Тема (раздел) учебной дисциплины	Виды учебной деятельности в часах/ в том числе интерактивной форме						Формы текущего контроля успеваемости и промежу-точной аттестации
			Л	ЛР	ПЗ/ТП	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
1	7	Раздел 1 Обеспечение информационной безопасности. контрольная работа №1)	6		4		10	20	ПК1
2	7	Раздел 2 Критерии оценки пригодности компьютерных систем TCSEC (Оранжевая книга). Критерии безопасности компьютерных систем CTCPEC.	8		4		10	22	
3	7	Раздел 3 Гармонизированные критерии оценки безопасности информационных технологий ITSEC.	8		4		10	22	
4	7	Раздел 4 Рекомендации X.800 для распределенных систем	8		2		12	22	ПК2, контрольная работа №2
5	7	Раздел 5 Общие критерии оценки безопасности информационных технологий.	6		4		12	22	
6	7	Раздел 7 Итоговая аттестация						0	ЗаО
7		Тема 1.1 Формальные методы доказательства правильности программ и их спецификаций							
8		Тема 1.2 Методы и средства анализа безопасности программного обеспечения (контрольно-испытательные методы логико-аналитические методы).							
9		Тема 1.3							

№ п/п	Семестр	Тема (раздел) учебной дисциплины	Виды учебной деятельности в часах/ в том числе интерактивной форме						Формы текущего контроля успеваемости и промежу-точной аттестации
			Л	ЛР	ПЗ/ТП	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
		Федеральные критерии безопасности информационных технологий.							
10		Тема 1.4 Защита АС и средств СВТ.							
11		Тема 1.5 Стандарты безопасности в сети Internet.							, (контрольная работа №1)
12		Тема 2.1 TCSEC (Основные группы безопасности) группа D, C, B, A. Классы безопасности (класс C1 - Discretionary Security Protection, класс C2 - Controlled Access Protection, класс B1 - Labeled Security Protection, класс B3 - Security Domains; класс A1							
13		Тема 2.2 TCPEC критерии конфиденциальности - контроль скрытых каналов; произвольное управление доступом; нормативное управление доступом; повторное использование объектов; критерии целостности - домены целостности; произвольное управление целостностью; нормативное управление целостностью; физическая целостность;							

№ п/п	Семестр	Тема (раздел) учебной дисциплины	Виды учебной деятельности в часах/ в том числе интерактивной форме						Формы текущего контроля успеваемости и промежу-точной аттестации
			Л	ЛР	ПЗ/ТП	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
		возможность осуществления отката; разделение ролей; самотестирование; критерии работоспособности - контроль за распределением ресурсов; устойчивость к отказам и сбоям; живучесть; восстановление; критерии аудита (регистрация и учет событий в системе; идентификация и аутентификация							
14		Тема 3.1 Гарантированность безопасности (семь возможных уровней гарантированности корректности - от E0 до E6; общая оценка системы). (группа D - Minimal Protection (минимальная защита); группа C - Discretionary Protection (избирательная защита); группа B - Mandatory Protection (полномочная защита) группа A - Verified Protection (проверяемая защита)).							
15		Тема 3.2 Сетевые конфигурации (требования к обеспечению конфиденциальности и целостности информации в сетевых конфигурациях). (класс C1 - Discretionary Security							

№ п/п	Семестр	Тема (раздел) учебной дисциплины	Виды учебной деятельности в часах/ в том числе интерактивной форме						Формы текущего контроля успеваемости и промежу-точной аттестации
			Л	ЛР	ПЗ/ТП	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
		Protection (избирательная защита безопасности) ; класс C2 - Controlled Access Protection (защита контролируемого доступа),класс B1 - Labeled Security Protection (меточная защита безопасности); класс B3 - Security Domains (области безопасности); класс A1 - Verified Desing (проверяемая разработка))							
16		Тема 4.1 Функции или сервисы безопасности (аутентификация; управление доступом; конфиденциальность данных; целостность данных; неотказуемость; реализация функций безопасности по уровням эталонной модели OSI).							
17		Тема 4.2 . Механизмы безопасности (шифрование; ЭП; дополнения трафика; управление маршрутизацией; нотаризация).							
18		Тема 4.3 Взаимосвязь функций и механизмов безопасности.							
19		Тема 4.4 Администрирование средств безопасности (администрирование системой; сервисами безопасности; механизмами							

№ п/п	Семестр	Тема (раздел) учебной дисциплины	Виды учебной деятельности в часах/ в том числе интерактивной форме						Формы текущего контроля успеваемости и промежу-точной аттестации
			Л	ЛР	ПЗ/ТП	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
		безопасности).							
20		Тема 5.1 Классификация набора требований безопасности (общие положения, структуры группирования и принципы целевого использования требований безопасности).							
21		Тема 5.2 Объект оценки (понятие, представление и общая модель).							
22		Тема 5.3 Требования безопасности (требования к функциям безопасности, требования гарантии безопасности).							
23		Тема 5.4 Критерии оценки для профилей защиты.							
24		Всего:	36		18		54	108	

4.4. Лабораторные работы / практические занятия

Лабораторные работы учебным планом не предусмотрены.

Практические занятия предусмотрены в объеме 18 ак. ч.

№ п/п	№ семестра	Тема (раздел) учебной дисциплины	Наименование занятий	Всего часов/ из них часов в интерактивной форме
1	2	3	4	5
1	7	РАЗДЕЛ 1 Обеспечение информационной безопасности.	Оценка технологической безопасности программного продукта.	4
2	7	РАЗДЕЛ 2 Критерии оценки пригодности компьютерных систем TCSEC (Оранжевая книга). Критерии безопасности компьютерных систем СТСРЕС.	Оценка безопасности информационной системы по критериям СТСРЕС.	4
3	7	РАЗДЕЛ 3 Гармонизированные критерии оценки безопасности информационных технологий ITSEC.	Оценка безопасности информационной системы по критериям TCSEC.	4
4	7	РАЗДЕЛ 4 Рекомендации X.800 для распределенных систем	Оценка безопасности информационной системы по общим критериям.	2
5	7	РАЗДЕЛ 5 Общие критерии оценки безопасности информационных технологий.	Оценка безопасности информационной системы по общим критериям.	4
			ВСЕГО:	18/0

4.5. Примерная тематика курсовых проектов (работ)

Курсовые проекты (работы) учебным планом не предусмотрены.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Преподавание дисциплины «Методы оценки безопасности компьютерных систем» осуществляется в форме лекций и практических занятий.
Лекции проводятся в традиционной классно-урочной организационной форме в объеме 18 часов, по типу управления познавательной деятельностью на 100% являются традиционными классически-лекционными (объяснительно-иллюстративными).
Практические работы (18 часов) организованы с использованием технологий развивающего обучения.
Самостоятельная работа студента организована с использованием традиционных видов работы. К традиционным видам работы (72 часа) относится отработка лекционного материала.
Весь курс разбит на 5 разделов, представляющих собой логически завершенный объем учебной информации. Фонды оценочных средств освоенных компетенций включают вопросы теоретического характера для оценки знаний. Теоретические знания проверяются путем применения таких организационных форм, как индивидуальные и групповые опросы.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

№ п/п	№ семестра	Тема (раздел) учебной дисциплины	Вид самостоятельной работы студента. Перечень учебно-методического обеспечения для самостоятельной работы	Всего часов
1	2	3	4	5
1	7	РАЗДЕЛ 1 Обеспечение информационной безопасности.	1. Изучение, анализ и дополнительная проработка лекционного материала по соответствующей теме. 2. Подготовка к практическому занятию №1. 3. Изучение учебной литературы из приведенных источников: [1, стр.50-74, [3, стр. 50-74], 1 [10-17].	10
2	7	РАЗДЕЛ 2 Критерии оценки пригодности компьютерных систем TCSEC (Оранжевая книга). Критерии безопасности компьютерных систем СТСРЕС.	1. Анализ и дополнительная проработка лекционного материала по соответствующей теме. 2. Подготовка к практическому занятию №2. 3. Изучение учебной литературы из приведенных источников: 1 [1, стр. 70-94], [2, стр.22-41].	10
3	7	РАЗДЕЛ 3 Гармонизированные критерии оценки безопасности информационных технологий ITSEC.	1. Изучение, анализ и дополнительная проработка лекционного материала по соответствующей теме. 2. Подготовка к практическому занятию №3. 3. Изучение учебной литературы из приведенных источников: [3, стр. 45-61].	10
4	7	РАЗДЕЛ 4 Рекомендации X.800 для распределенных систем	Изучение, анализ и дополнительная проработка лекционного материала по соответствующей теме . Подготовка к практическому занятию № 4. 3. Подготовка к контрольной работе № 2. 4. Изучение учебной литературы из приведенных источников: [1, стр.40-58], [2, стр.38-40, 144-165] [3, стр.45-61].	12
5	7	РАЗДЕЛ 5 Общие критерии оценки безопасности информационных технологий.	1. Дополнительная проработка лекционного материала по соответствующей теме. 2. Подготовка к практическому занятию №5. 3. Изучение учебной литературы из приведенных источников: [1, стр. 221-235], [3, стр.45-61], [4, стр.98-130].	12
			ВСЕГО:	54

7. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1. Основная литература

№ п/п	Наименование	Автор (ы)	Год и место издания Место доступа	Используется при изучении разделов, номера страниц
1	Информационная безопасность и защита информации	В.П. Мельников, С.А. Клейменов, А.М. Петраков	МИИТ НТБ, 2012 НТБ МИИТ	2 [22-41],
2	Защита информации	В. П. Мельников, А. И. Куприянов, А. Г. Схиртладзе	М.: Академия, 304с. МИИТ НТБ (004 М48), 2014 НТБ МИИТ	1 [50-74],4[45-61]
3	Оценка уровня информационной безопасности на объекте информатизации: учебное пособие для студ. вузов ж.-д. трансп.	К.А. Паршин.	М.: ФГБОУ "УМЦ ЖДТ", 95с. МИИТ НТБ, 2014 НТБ МИИТ	1 [50-74],4[45-61]

7.2. Дополнительная литература

№ п/п	Наименование	Автор (ы)	Год и место издания Место доступа	Используется при изучении разделов, номера страниц
4	Технические, организационные и кадровые аспекты управления информационной безопасностью.	Милославская Н., Сенаторов М., Толстой А.	М.:Горячая линия , 2014 НТБ МИИТ	1 [10-17],

8. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ "ИНТЕРНЕТ", НЕОБХОДИМЫЕ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

• Форум специалистов по информационным технологиям http://citforum.ru/
• Интернет-университет информационных технологий http://www.intuit.ru/
• Электронный фонд правовой и нормативно-технической документацииhttp://docs.cntd.ru/
• ГОСТ РФ http://gostrf.com/
• http://dehack.ru
• www.securitylab.ru

9. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Microsoft Windows
Microsoft Office

Putty
Бесплатноеиспользование (MIT)

10. ОПИСАНИЕ МАТЕРИАЛЬНО ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Учебная аудитория для проведения занятий лекционного типа, групповых и индивидуальных консультаций
№1329
Аудиовизуальное оборудование для аудитории, АРМ управляющий, проектор, экран проекционный Аудитория подключена к интернету МИИТ.
Учебная аудитория для проведения практических занятий №1327
Рабочие станции для студентов 17шт, коммутатор CISCO – 9шт, маршрутизатор CISCO – 9шт, сетевое оборудование, рабочая станция преподавателя, проектор, экран, доска

11. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Студентам необходимо помнить, что качество полученного образования в немалой степени зависит от активной роли самого обучающегося в учебном процессе. Студент должен быть нацелен на максимальное усвоение подаваемого лектором материала, после лекции и вовремя специально организуемых индивидуальных встреч он может задать лектору интересующие его вопросы.
Лекционные занятия (18 часов) составляют основу теоретического обучения и должны давать систематизированные основы знаний по дисциплине, раскрывать состояние и перспективы развития соответствующей области науки, концентрировать внимание обучающихся на наиболее сложных и узловых вопросах, стимулировать их активную познавательную деятельность и способствовать формированию творческого мышления.
Главная задача лекционного курса – сформировать у студентов системное представление об изучаемом предмете, обеспечить усвоение основополагающего учебного материала, принципов и закономерностей развития соответствующей научно-практической области, а также методов применения полученных знаний, умений и навыков.
Основные функции лекций:
- познавательно-обучающая;
- развивающая;
- ориентирующе-направляющая;
- активизирующая;
- воспитательная;
- организующая;
- информационная.

Выполнение практических занятий служит важным связующим звеном между теоретическим освоением данной дисциплины и применением ее положений на практике. Они способствуют развитию самостоятельности обучающихся, более активному освоению учебного материала, являются важной предпосылкой формирования профессиональных качеств бакалавров. Практические занятия (18 часов) организованы с использованием технологий развивающего обучения. Проведение практических занятий не сводится только к органичному дополнению лекционных курсов и самостоятельной работы студентов. Практические занятия следует рассматривать как важное средство проверки усвоения обучающимися тех или иных положений, даваемых на лекции, а также рекомендуемой для изучения литературы. Задачи практических занятий – закрепление и углубление знаний, полученных на лекциях и приобретенных в процессе самостоятельной работы с учебной литературой, формирование у обучающихся умений и навыков работы с исходными данными, научной литературой и специальными документами. Практическому занятию должно предшествовать ознакомление с лекцией на соответствующую тему и литературой, указанной в плане этих занятий.

Самостоятельная работа (72 часа) может быть успешной при определенных условиях, которые необходимо организовать. Ее правильная организация, включающая технологии отбора целей, содержания, конструирования заданий и организацию контроля, систематичность самостоятельных учебных занятий, целесообразное планирование рабочего времени позволяет привить студентам умения и навыки в овладении, изучении, усвоении и систематизации приобретаемых знаний в процессе обучения, привить навыки повышения профессионального уровня в течение всей трудовой деятельности.
Каждому студенту следует составлять еженедельный семестровый план работы, а также план на каждый учебный день. Нужно осуществлять самоконтроль, который является необходимым условием успешной работы. Если что-то осталось невыполненным, необходимо изыскать время для завершения этой части работы, не уменьшая объема недельного плана.
Компетенции обучающегося, формируемые в результате освоения учебной дисциплины, рассмотрены через соответствующие знания, умения и владения. Для проверки уровня освоения дисциплины предлагаются вопросы к зачету с оценкой; практические и контрольные работы, где каждый вариант содержит задания, разработанные в рамках основных тем учебной дисциплины и включающие терминологические задания; вопросы к защите практических и контрольных работ.
Фонд оценочных средств является составной частью учебно-методического обеспечения процедуры оценки качества освоения образовательной программы и обеспечивает повышение качества образовательного процесса и входит, как приложение, в состав рабочей программы дисциплины.
Основные методические указания для обучающихся по дисциплине указаны в разделе основная и дополнительная литература.