

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА
 Федеральное государственное бюджетное образовательное учреждение
 высшего образования
 "Уральский государственный университет путей сообщения"
 (ФГБОУ ВО УрГУПС)

Б1.Б.24 Теория информационной безопасности и методология защиты информации рабочая программа дисциплины (модуля)

Закреплена за кафедрой Учебный план	Информационные технологии и защита информации 10.03.01 ИБ-2020.plx Направление подготовки 10.03.01 Информационная безопасность Направленность (профиль) "Организация и технология защиты информации (на транспорте)"		
Направленность (профиль)	направленность (профиль) N 2 "Организация и технология защиты информации" (по отрасли или в сфере профессиональной деятельности)		
Квалификация	Бакалавр		
Форма обучения	очная		
Объем дисциплины (модуля)	4 ЗЕТ		
Часов по учебному плану в том числе:	144	Часов контактной работы всего, в том числе:	38,05
аудиторные занятия	36	аудиторная работа	36
самостоятельная работа	108	текущие консультации по практическим занятиям	1,8
Промежуточная аттестация и формы контроля:		прием зачета с оценкой	0,25
зачет с оценкой 4			

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	4 (2.2)		Итого	
	18			
Неделя	УП	РПД	УП	РПД
Лекции	18	18	18	18
Практические	18	18	18	18
Контактная работа	36	36	36	36
Итого ауд.	36	36	36	36
Сам. работа	108	108	108	108
Итого	144	144	144	144

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Системно изложить современный подход к вопросам информационной безопасности и защиты информации в Российской Федерации.
1.2	Обучить студентов системно использовать и применять основные принципы и методологии построения эффективных систем защиты информации.
1.3	Ознакомить студентов с нормативно-правовой базой, действующей в данной предметной области.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОП

Цикл (раздел) ОП:	Б1.Б
2.1 Требования к предварительной подготовке обучающегося:	
Для изучения данной учебной дисциплины необходимы знания, умения и навыки, приобретенные в ходе изучения дисциплины Основы информационной безопасности. В результате освоения предшествующих дисциплин обучающийся должен знать: место и роль информационной безопасности в системе национальной безопасности; уметь: анализировать и оценивать угрозы информационной безопасности объекта; пользоваться нормативными документами по защите информации; владеть: навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности; профессиональной терминологией.	
2.2 Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:	
Управление информационной безопасностью на объектах транспортной инфраструктуры Комплексные системы защиты информации на транспорте Защита информационных процессов на транспорте	

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

ОПК-7: способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	
Знать:	
Уровень 1	классификацию защищаемой информации
Уровень 2	классификацию угроз защищаемой информации
Уровень 3	возможные методы и пути реализации угроз защищаемой информации
Уметь:	
Уровень 1	выявлять угрозы информационной безопасности объекта
Уровень 2	анализировать угрозы информационной безопасности объекта
Уровень 3	оценивать угрозы информационной безопасности объекта
Владеть:	
Уровень 1	методами и средствами выявления угроз информационной безопасности объекта
Уровень 2	методами и средствами анализа информационной безопасности объекта
Уровень 3	методами и средствами оценки информационной безопасности объекта

ПК-4: способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты

Знать:	
Уровень 1	цели, задачи, принципы и основные направления обеспечения информационной безопасности государства; основные термины по проблематике информационной безопасности; методологию создания систем защиты информации; перспективные направления развития средств и методов защиты информации; роль и место информационной безопасности в системе национальной безопасности
Уровень 2	цели, задачи, принципы и основные направления обеспечения информационной безопасности государства; основные термины по проблематике информационной безопасности; перспективные направления развития средств и методов защиты информации; роль и место информационной безопасности в системе национальной безопасности; компьютерную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности; особенности обеспечения информационной безопасности компьютерных систем при обработке информации, составляющей государственную тайну
Уровень 3	перспективные направления развития средств и методов защиты информации; роль и место информационной безопасности в системе национальной безопасности; компьютерную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности; особенности обеспечения информационной безопасности компьютерных систем при обработке информации, составляющей государственную тайну; современные подходы к построению систем защиты информации

Уметь:	
Уровень 1	пользоваться современной научно-технической информацией по исследуемым проблемам и задачам
Уровень 2	пользоваться современной научно-технической информацией по исследуемым проблемам и задачам; выбирать и анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации
Уровень 3	пользоваться современной научно-технической информацией по исследуемым проблемам и задачам; выбирать и анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации; разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации; разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации
Владеть:	
Уровень 1	навыками формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем; навыками работы с нормативными правовыми актами; навыками организации и обеспечения режима секретности
Уровень 2	навыками формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем; навыками работы с нормативными правовыми актами; навыками организации и обеспечения режима секретности; методами организации и управления деятельностью служб по защите информации на предприятии
Уровень 3	навыками формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем; навыками работы с нормативными правовыми актами; навыками организации и обеспечения режима секретности; методами организации и управления деятельностью служб по защите информации на предприятии; навыками анализа информационной инфраструктуры информационной системы и её безопасности; методами мониторинга и аудита, выявления угроз информационной безопасности

В результате освоения дисциплины обучающийся должен

3.1	Знать:
3.1.1	направления обеспечения информационной безопасности государства;
3.1.2	основные термины по проблематике информационной безопасности;
3.1.3	методологию создания систем защиты информации;
3.1.4	перспективные направления развития средств и методов защиты информации;
3.1.5	роль и место информационной безопасности в системе национальной безопасности;
3.1.6	основы организационного и правового обеспечения информационной безопасности;
3.1.7	классификацию защищаемой информации; классификацию угроз защищаемой информации.
3.2	Уметь:
3.2.1	выбирать показатели качества и критерии оценки систем и средств защиты информации;
3.2.2	пользоваться современной научно-технической информацией по вопросам безопасности;
3.2.3	определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; разрабатывать модели угроз и модели нарушителей информационной безопасности выявлять уязвимости информационных ресурсов, проводить мониторинг угроз информационной безопасности.
3.3	Владеть:
3.3.1	навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности;
3.3.2	навыками обоснования, выбора, реализации и контроля результатов управленческого решения;
3.3.3	навыками формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем;
3.3.4	навыками работы с нормативными правовыми актами; навыками организации и обеспечения режима секретности.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов (академических)	Компетенции	Литература	Активные формы
	Раздел 1. Концептуальные понятия информационной безопасности					
1.1	Закон Российской Федерации "О безопасности". Концепция национальной безопасности Российской Федерации. Доктрина информационной безопасности Российской Федерации /Лек/	4	2	ОПК-7	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2	

1.2	Подготовка к практическим занятиям /Ср/	4	4	ПК-4	Л1.1 Л1.2Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13 Л3.1 Л3.2 Э1 Э2	
1.3	Сущность и понятие информационной безопасности, характеристика ее составляющих. Значение информационной безопасности для субъектов информационных отношений /Пр/	4	2	ПК-4	Л1.1 Л1.2Л2.2Л3.2 Э1 Э2	Групповая дискуссия
1.4	Федеральный закон «Об информации, информационных технологиях и о защите информации». Закон Российской Федерации «О государственной тайне» /Лек/	4	2	ОПК-7	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2	
1.5	Подготовка к практическим занятиям /Ср/	4	4	ПК-4	Л1.1 Л1.2Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13 Л3.1 Л3.2 Э1 Э2	
1.6	Понятие и сущность защиты информации. Защищаемая информация – основные свойства и состав. Место защиты информации в системе информационной безопасности РФ. Классификация информации ограниченного доступа /Пр/	4	2	ПК-4	Л1.1 Л1.2Л2.2Л3.2 Э1 Э2	Групповая дискуссия
1.7	План защиты информации на предприятии /Пр/	4	4	ПК-4	Л1.1 Л1.2Л2.2Л3.2 Э1 Э2	Групповая дискуссия
1.8	Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации /Лек/	4	2	ОПК-7	Л1.1 Л1.2 Л1.3Л2.2 Э1 Э2	
1.9	Подготовка к практическим занятиям /Ср/	4	4	ПК-4	Л1.1 Л1.2Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13 Л3.1 Л3.2 Э1 Э2	
1.10	Методологические подходы к защите информации и принципы ее организации. Объекты защиты. Виды защиты. Классификация методов и средств защиты информации /Пр/	4	4	ПК-4	Л1.1 Л1.2Л2.2Л3.2 Э1 Э2	Групповая дискуссия

1.11	Изучение литературы по тематике раздела /Ср/	4	28	ОПК-7	Л1.1 Л1.2 Л1.3Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13 Л3.1 Л3.2 Э1 Э2	
	Раздел 2. Технология создания политики безопасности					
2.1	Дискреционный принцип разграничения доступа /Лек/	4	2	ОПК-7	Л1.1 Л1.2 Л1.3Л2.2 Э1 Э2	
2.2	Мандатный принцип разграничения доступа (нормативный) /Лек/	4	2	ОПК-7	Л1.1 Л1.2 Л1.3Л2.2 Э1 Э2	
2.3	Классическая модель Бел Ла Падулы /Лек/	4	2	ОПК-7	Л1.1 Л1.2 Л1.3Л2.2 Э1 Э2	
2.4	Уполномоченные субъекты в моделях, реализующих мандатный доступ /Лек/	4	2	ОПК-7	Л1.1 Л1.2 Л1.3Л2.2 Э1 Э2	
2.5	Безопасная функция перехода модели совместного доступа /Лек/	4	2	ОПК-7	Л1.1 Л1.2 Л1.3Л2.2 Э1 Э2	
2.6	Модель совместного доступа с уполномоченными субъектами. Рольевая политика доступа /Лек/	4	2	ОПК-7	Л1.1 Л1.2 Л1.3Л2.2 Э1 Э2	
2.7	Подготовка к практическим занятиям /Ср/	4	4	ПК-4	Л1.1 Л1.2Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13 Л3.1 Л3.2 Э1 Э2	
2.8	Понятие и сущность защиты информации. Защищаемая информация – основные свойства и состав. Место защиты информации в системе информационной безопасности РФ. Классификация информации ограниченного доступа /Пр/	4	6	ПК-4	Л1.1 Л1.2Л2.2Л3.2 Э1 Э2	Групповая дискуссия
2.9	Изучение литературы по тематике раздела /Ср/	4	28	ОПК-7	Л1.1 Л1.2 Л1.3Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13 Л3.1 Л3.2 Э1 Э2	
2.10	Подготовка к промежуточной аттестации /Ср/	4	36	ОПК-7 ПК-4	Л1.1 Л1.2 Л1.3Л2.2Л3.1 Л3.2 Э1 Э2	

5. ФОНД ОЦЕНОЧНЫХ МАТЕРИАЛОВ

Фонд оценочных материалов по дисциплине, состоящий из ФОМ для текущего контроля и проведения промежуточной аттестации обучающихся, разрабатывается по каждой дисциплине и хранится на кафедре. Оценочные материалы дублируются на странице данного курса в системе электронной поддержки обучения Blackboard Learn (сайт bb.usurt.ru), доступной через личный кабинет обучающегося.

Фонд оценочных материалов для проведения промежуточной аттестации обучающихся по дисциплине (модулю), включая порядок проведения промежуточной аттестации, систему оценивания результатов промежуточной аттестации и критерии выставления оценок, примеры типовых заданий или иных материалов, необходимых для оценки знаний, умений, навыков, используемых для промежуточной аттестации по дисциплине, приведен в приложении 1 к рабочей программе дисциплины.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1 Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

6.1.1. Основная учебная литература

	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
Л1.1	Баранова Е. К., Бабаш А. В.	Информационная безопасность и защита информации: Учебное пособие	Москва: Издательский Центр РИО❖, 2017	http://znanium.com
Л1.2	Ададуров С. Е., Корниенко А. А.	Информационная безопасность и защита информации на железнодорожном транспорте: В 2ч. Ч.1: Методология и система обеспечения информационной безопасности на железнодорожном транспорте: Учебник	Москва: ФГБОУ "Учебно-методический центр по образованию на железнодорожном транспорте" (УМЦ ЖДТ), 2014	http://znanium.com
Л1.3	Паршин К. А.	Теория информационной безопасности и методология защиты информации: конспект лекций для студентов направления подготовки 10.03.01 «Информационная безопасность»	Екатеринбург: УрГУПС, 2016	http://biblioserver.usurt.ru/cgi-bin/irbis64r_13/cgiirbis_64.exe?C21COM=F&I21DBN=KN&P21DBN=KN

6.1.2. Дополнительная учебная литература

	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
Л2.1		Кодексы и Законы Российской Федерации: официальное издание	СПб.: Весь, 2007	
Л2.2	Мельников В. П., Клейменов С. А., Петраков А. М., Клейменов С. А.	Информационная безопасность и защита информации: учебное пособие для студентов вузов, обучающихся по специальности 230201 - "Информационные системы и технологии"	Москва: Академия, 2009	
Л2.3		Федеральный закон от 28 декабря 2010 г. N 390-ФЗ «О безопасности» (с изменениями и дополнениями)		http://www.consultant.ru/document/cons_doc_LAW_108546/
Л2.4		Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями и дополнениями)		http://www.consultant.ru/document/cons_doc_LAW_61798/
Л2.5		Закон РФ от 21 июля 1993 г. N 5485-1 «О государственной тайне» (с изменениями и дополнениями)		http://www.consultant.ru/document/cons_doc_LAW_2481/
Л2.6		Указ Президента РФ от 6 марта 1997 г. N 188 "Об утверждении перечня сведений конфиденциального характера" (с изменениями и дополнениями)		http://www.consultant.ru/document/cons_doc_LAW_13532/

Л2.7		Руководящий документ «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации»	Утв. Гостехкомиссией России, 30.03.1992 г.	http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=OTN&n=19095#04821573941739876
Л2.8		Защита информации. Инсайд: специализированное отечественное периодическое издание	Издательский Дом «Афина»	https://elibrary.ru/title_about.asp?id=25917
Л2.9		Вестник УрФО. Безопасность в информационной сфере: специализированное отечественное периодическое издание	Изд-во ЮУрГУ	https://elibrary.ru/title_about.asp?id=32751
Л2.10		Безопасность информационных технологий: специализированное отечественное периодическое издание	Изд-во Национального исследовательского ядерного университета «МИФИ»	https://elibrary.ru/title_about.asp?id=8429
Л2.11		Information and Computer Security: специализированное зарубежное периодическое издание	Emerald	https://www.scopus.com/sourceid/21100421900?origin=resultlist
Л2.12		Information Security Journal: специализированное зарубежное периодическое издание	Taylor & Francis	https://www.scopus.com/sourceid/19700187807?origin=resultlist
Л2.13		Каталог учебных, учебно-методических пособий, научных и других изданий вузов железнодорожного транспорта: справочно-библиографическое издание	Москва, ФГБУ ДПО «УМЦ ЖДТ» 2018	http://www.usurt.ru/izdatelsko-bibliotechnyy-kompleks/bibliotechno-informacionnuy-center/katalog-fgbou-umts-zhdt

Нормативные методические документы в области информационной безопасности при изучении данной дисциплины не используются

6.1.3. Методические разработки

	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
Л3.1	Зырянова Т. Ю., Ганженко Н.	Теория информационной безопасности и методология защиты информации: методические рекомендации к самостоятельной работе студентов направления подготовки 10.03.01 «Информационная безопасность»	Екатеринбург: УрГУПС, 2016	http://biblioserver.usurt.ru/cgi-bin/irbis64r_13/cgiirbis_64.exe?C21COM=F&I21DBN=KN&P21DBN=KN
Л3.2	Зырянова Т. Ю.	Теория информационной безопасности и методология защиты информации: методические рекомендации по подготовке к практическим семинарам для студентов направления подготовки 10.03.01 «Информационная безопасность»	Екатеринбург: УрГУПС, 2016	http://biblioserver.usurt.ru/cgi-bin/irbis64r_13/cgiirbis_64.exe?C21COM=F&I21DBN=KN&P21DBN=KN

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)

Э1	Официальный сайт Федеральной службы по техническому и экспортному контролю Российской Федерации (http://www.fstec.ru)
Э2	Система электронной поддержки обучения Blackboard Learn (http://bb.usurt.ru)

6.3 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем

6.3.1 Перечень программного обеспечения

6.3.1.1	Неисключительные права на ПО Windows
6.3.1.2	Неисключительные права на ПО Office
6.3.1.3	Система электронной поддержки обучения Blackboard Learn

6.3.2 Перечень информационных справочных систем и профессиональных баз данных

6.3.2.1	Справочно-правовая система КонсультантПлюс
6.3.2.2	Справочно-правовая система Гарант
6.3.2.3	Автоматизированная система правовой информации на железнодорожном транспорте АСПИ ЖТ (профессиональная БД)

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Назначение	Оснащение
Учебная аудитория для проведения текущего контроля и промежуточной аттестации	Специализированная мебель
Учебная аудитория для проведения занятий лекционного типа	Специализированная мебель Демонстрационное оборудование - Комплект мультимедийного оборудования Учебно-наглядные пособия - презентационные материалы
Компьютерный класс - Учебная аудитория для самостоятельной работы студентов	Специализированная мебель Компьютерная техника с установленным лицензионным ПО, предусмотренным пунктом 6.3.1 РПД, с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Университета
Учебная аудитория для проведения групповых и индивидуальных консультаций	Специализированная мебель
Читальный зал Информационно-	Специализированная мебель Компьютерная техника с возможностью подключения к сети "Интернет" и обеспечением
библиотечного центра ИБК УрГУПС - Аудитория для самостоятельной работы Компьютерный класс - Учебная аудитория для проведения практических (занятий семинарского типа) и лабораторных занятий, групповых и индивидуальных консультаций	доступа в электронную информационно-образовательную среду Университета Специализированная мебель Компьютерная техника с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Университета Технические средства обучения - Комплект мультимедийного оборудования

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ) И ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Эффективное освоение дисциплины предполагает регулярное посещение всех видов аудиторных занятий, выполнение плана самостоятельной работы в полном объеме и прохождение аттестации в соответствии с календарным учебным графиком.

Студенту рекомендуется ознакомиться со списком основной и дополнительной литературы и взять в библиотеке издания (необходимо иметь при себе персонифицированную электронную карту и уметь пользоваться электронным каталогом «ИРБИС»).

Доступ к информационным ресурсам библиотеки и информационно-справочным системам сети «Интернет» организован в читальных залах библиотеки, в компьютерных классах, в помещениях для самостоятельной работы студентов со стационарных ПЭВМ, либо с личного ПЭВМ (ноутбука, планшетного компьютера или иного мобильного устройства) посредством беспроводного доступа при активации индивидуальной учетной записи.

Пользование информационными ресурсами расширяет возможности освоения теоретического курса, выполнения самостоятельной работы и позволяет получить информацию для реализации творческих образовательных технологий.

Комплект учебно-методических материалов по всем видам учебной деятельности, предусмотренным рабочей программой дисциплины (модуля), размещен на странице данного курса в системе электронной поддержки обучения Blackboard Learn (сайт bb.usurt.ru), доступной через личный кабинет обучающегося.

Методические материалы, разработанные для обеспечения образовательного процесса представлены в электронном каталоге УрГУПС.

Формы самостоятельной работы студентов по данной дисциплине разнообразны. Они включают в себя:

- изучение лекционного и дополнительного материала (учебной, научной, методической литературы, материалов периодических изданий);
- подготовку к занятиям, предусмотренных РПД, мероприятиям текущего контроля и промежуточной аттестации

Выполнять самостоятельную работу и отчитываться по ее результатам студент должен в соответствии с календарным планом изучения дисциплины, видами и сроками отчетности.

При выполнении самостоятельной работы студент должен руководствоваться методическими указаниями, размещенными на странице данного курса в системе электронной поддержки обучения Blackboard Learn (сайт bb.usurt.ru), а также учебно-методическими материалами, которые указаны для СРС по темам дисциплины в разделе 4 РПД "Структура и содержание дисциплины (модуля)".

Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине указан по темам дисциплины в разделе 4 РПД "Структура и содержание дисциплины (модуля)", материалы размещены на странице данного курса в системе электронной поддержки обучения Blackboard Learn (сайт bb.usurt.ru).

