ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

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

Б1.Б.15 Основы управления информационной безопасностью

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Информационные технологии и защита информации**

Учебный план 10.03.01 ИБ-2023.plx
10.03.01 Информационная безопасность

Направленность (профиль) Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)

Квалификация **Бакалавр**

Форма обучения **очная**

Объем дисциплины (модуля) **4 ЗЕТ**

Часов по учебному плану 144
в том числе:
аудиторные занятия 36
самостоятельная работа 36
часов на контроль 36

Часов контактной работы всего, в том числе: 40,3
аудиторная работа 36
текущие консультации по практическим занятиям 1,8
консультации перед экзаменом 2
прием экзамена 0,5

Промежуточная аттестация и формы контроля:
экзамен 6

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**6 (3.2)**		Итого	
Недель	18			
Вид занятий	УП	РП	УП	РП
Лекции	18	18	18	18
Практические	18	18	18	18
Элект	36	36	36	36
Итого ауд.	36	36	36	36
Контактная работа	72	72	72	72
Сам. работа	36	36	36	36
Часы на контроль	36	36	36	36
Итого	144	144	144	144

1. ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Цель дисциплины: Изучение основных понятий, методологии и практических приемов управления технической и организационной инфраструктурой обеспечения информационной безопасности на предприятии.
1.2	Задачи дисциплины:
1.3	Приобретение обучаемыми необходимого объема знаний и практических навыков в области стандартизации в управлении информационной безопасностью.
1.4	Формирование у обучаемых целостного представления об организации и содержании процессов управления информационной безопасностью на предприятии как результата внедрения системного подхода к решению задач обеспечения информационной безопасности.

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 Теория информационной безопасности и методология защиты информации.
В результате освоения предшествующих дисциплин обучающийся должен знать: основы российской правовой системы и законодательства; основные понятия и методы в управленческой деятельности; место и роль информационной безопасности в системе национальной безопасности Российской Федерации; методологию создания систем защиты информации;
уметь: использовать в практической деятельности правовые знания; оценивать эффективность управленческих решений; анализировать и оценивать угрозы информационной безопасности объекта; выбирать показатели качества и критерии оценки систем и средств защиты информации; пользоваться современной научно-технической информацией по вопросам безопасности; 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;
владеть: навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности; навыками обоснования, выбора, реализации и контроля результатов управленческого решения; профессиональными способами обеспечения безопасности в сфере информации; профессиональной терминологией в области информационной безопасности.

2.2 Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:

Производственная практика (эксплуатационная практика)
Производственная практика (преддипломная практика)
Производственная практика (технологическая практика)
Управление информационной безопасностью на объектах транспортной инфраструктуры

Подготовка к сдаче и сдача государственного экзаменаПодготовка к процедуре защиты и защита выпускной квалификационной работы

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ
УК-2: Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений
УК-2.1: Формулирует в рамках поставленной цели проекта совокупность задач, обеспечивающих ее достижение
УК-2.2: Определяет потребности в ресурсах для решения задач профессиональной деятельности
УК-2.3: Выбирает оптимальный способ решения задач, учитывая действующие правовые нормы и имеющиеся условия, ресурсы и ограничения
ОПК-5: Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности;
ОПК-5.2: Применяет нормативные правовые акты и нормативные методические документы по информационной безопасности в профессиональной деятельности
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;
ОПК-10.1: Знает требования к формированию политики информационной безопасности и управлению информационной безопасностью на объекте защиты
ОПК-10.2: Классифицирует информационную систему по требованиям защиты информации
ОПК-10.3: Определяет угрозы безопасности информации, реализация которых может привести к нарушению безопасности информации в компьютерной системе и сети
ОПК-10.4: Формирует комплекс мер по противодействию угрозам информационной безопасности, организовывает и поддерживает его выполнение

ОПК-12: Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений;
ОПК-12.2: Анализирует, проверяет достоверность, полноту, актуальность и непротиворечивость данных и содержательно интерпретирует полученные результаты для технико-экономического обоснования проектных решений
ОПК-2.1: Способен проводить анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба;
ОПК(п)-2.1.2: Выявляет источники информационных угроз, их возможные цели, пути реализации
ОПК(п)-2.1.1: Знает функциональные процессы и информационные составляющие объектов защиты
ОПК(п)-2.1.3: Оценивает предполагаемый ущерб от реализации информационных угроз
ОПК-2.3: Способен разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности;
ОПК(п)-2.3.2: Знает и применяет международные и национальные стандарты в области информационной безопасности

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации;
3.1.2	принципы организации информационных систем в соответствии с требованиями по защите информации;
3.1.3	основные нормативные правовые акты в области информационной безопасности и защиты информации.
3.2	**Уметь:**
3.2.1	анализировать и оценивать угрозы информационной безопасности объекта;
3.2.2	применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем;
3.2.3	пользоваться нормативными документами по защите информации;
3.2.4	формулировать и настраивать политику безопасности распространенных операционных систем, а также вычислительных сетей, построенных на их основе.
3.3	**Владеть:**
3.3.1	навыками работы с нормативными правовыми актами;
3.3.2	навыками работы с нормативными документами;
3.3.3	методами и средствами выявления угроз безопасности автоматизированным системам;
3.3.4	методами формирования требований по защите информации;
3.3.5	методами анализа и формализации информационных процессов объекта и связей между ними;
3.3.6	методами организации и управления деятельностью служб защиты информации на предприятии;
3.3.7	методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов (академических)	Компетенции	Литература	Активные формы
	Раздел 1. Введение в системы управления информационной безопасностью					
1.1	Системный подход к управлению информационной безопасностью /Лек/	6	2		Л1.1Л2.1 Л2.2 Э2 Э3 Э4	
1.2	Классификация понятий в области информационной безопасности и защиты информации /Пр/	6	2	ОПК-5.2	Л1.1Л2.1 Л2.2Л3.2 Э2 Э3 Э4	Работа в группе. Изучение нормативных правовых документов
1.3	Изучение литературы и нормативных правовых документов по тематике раздела, выполнение заданий по практическим занятиям /Ср/	6	12	ОПК-5.2	Л1.1Л2.1 Л2.2Л3.1 Э2 Э3 Э4	

	Раздел 2. Управление информационными рисками как базовый процесс системы управления информационной безопасностью					
2.1	Стандарты серии ГОСТ Р ИСО/МЭК 27000. Теоретические основы управления информационными рисками /Лек/	6	2		Л1.1Л2.1 Л2.2 Э2 Э3 Э4	
2.2	Введение в информационно-аналитические системы. Метод регрессионного анализа с использованием системы STATISTICA /Пр/	6	2		Л1.1Л2.1 Л2.2Л3.2 Э2 Э3 Э4	Работа в группе. Решение практических задач с применением прикладного программного обеспечения
2.3	Теоретические основы анализа временных рядов /Лек/	6	2		Л1.1Л2.1 Л2.2 Э2 Э3 Э4	
2.4	Решение задачи прогнозирования информационного риска методом анализа временных рядов в системе STATISTICA /Пр/	6	2	УК-2.1	Л1.1Л2.1 Л2.2Л3.2 Э2 Э3 Э4	Работа в группе. Решение практических задач с применением прикладного программного обеспечения
2.5	Обзор интеллектуальных методов анализа данных /Лек/	6	2		Л1.1Л2.1 Л2.2 Э2 Э3 Э4	
2.6	Примеры интеллектуального анализа данных в системе STATISTICA /Пр/	6	2	УК-2.1	Л1.1Л2.1 Л2.2Л3.2 Э2 Э3 Э4	Работа в группе. Решение практических задач с применением прикладного программного обеспечения
2.7	Основы теории нечетких множеств и нечеткой логики /Лек/	6	2		Л1.1Л2.1 Л2.2 Э2 Э3 Э4	
2.8	Анализ информационного риска на основе теории нечетких множеств в системе Matlab /Пр/	6	2	УК-2.1	Л1.1Л2.1 Л2.2Л3.2 Э2 Э3 Э4	Работа в группе. Решение практических задач с применением прикладного программного обеспечения
2.9	Изучение литературы и нормативных правовых документов по тематике раздела, выполнение заданий по практическим занятиям /Ср/	6	12	УК-2.1	Л1.1Л2.1 Л2.2Л3.1 Э2 Э3 Э4	
	Раздел 3. Управление информационной безопасностью в отдельных классах информационных систем					
3.1	Стандарт ГОСТ Р ИСО/МЭК 15408. Профили защиты. Современная система сертификации средств защиты информации /Лек/	6	2		Л1.1Л2.1 Л2.2 Э2 Э3 Э4	
3.2	Управление информационной безопасностью в государственных информационных системах /Пр/	6	2	ОПК-5.2 ОПК-10.1 ОПК-10.2 ОПК-10.4 ОПК-12.2	Л1.1Л2.1 Л2.2Л3.2 Э2 Э3 Э4	Работа в группе. Применение нормативных правовых документов

3.3	Методика оценки угроз безопасности информации /Лек/	6	2	ОПК-10.1	Л1.1Л2.1 Л2.2 Э2 Э3 Э4	
3.4	Построение модели угроз безопасности для государственной информационной системы /Пр/	6	2	УК-2.1 УК-2.2 УК-2.3 ОПК-5.2 ОПК-10.1 ОПК-10.3	Л1.1Л2.1 Л2.2Л3.2 Э2 Э3 Э4	Работа в группе. Применение нормативных правовых документов
3.5	Законодательные основы обеспечения безопасности персональных данных /Лек/	6	2	ОПК-10.1	Л1.1Л2.1 Л2.2 Э2 Э3 Э4	
3.6	Управление информационной безопасностью в информационных системах персональных данных /Пр/	6	2	УК-2.1 УК-2.2 УК-2.3 ОПК-5.2 ОПК-10.1 ОПК-10.2 ОПК-10.4 ОПК-12.2	Л1.1Л2.1 Л2.2Л3.2 Э2 Э3 Э4	Работа в группе. Применение нормативных правовых документов
3.7	Критическая информационная инфраструктура Российской Федерации /Лек/	6	2	ОПК-10.1	Л1.1Л2.1 Л2.2 Э2 Э3 Э4	
3.8	Управление информационной безопасностью на значимых объектах критической информационной инфраструктуры Российской Федерации /Пр/	6	2	УК-2.1 УК-2.2 УК-2.3 ОПК-5.2 ОПК-10.1 ОПК-10.2 ОПК-10.4 ОПК-12.2	Л1.1Л2.1 Л2.2Л3.2 Э2 Э3 Э4	Работа в группе. Применение нормативных правовых документов
3.9	Изучение литературы и нормативных правовых документов по тематике раздела, выполнение заданий по практическим занятиям /Ср/	6	12	УК-2.1 УК-2.2 УК-2.3 ОПК-5.2 ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-10.4 ОПК-12.2	Л1.1Л2.1 Л2.2Л3.1 Э2 Э3 Э4	
3.10	Взаимодействие с обучающимися по вопросам текущего контроля в электронной информационно-образовательной среде: выполнение контрольных заданий и промежуточных тестов /Элект/	6	36	УК-2.1 УК-2.2 УК-2.3 ОПК-5.2 ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-10.4 ОПК-12.2	Л1.1Л2.1 Л2.2Л3.1 Л3.2 Э2 Э3 Э4	
3.11	Промежуточная аттестация /Экзамен/	6	36	УК-2.1 УК-2.2 УК-2.3 ОПК-5.2 ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-10.4 ОПК-12.2	Л1.1Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	

5. ФОНД ОЦЕНОЧНЫХ МАТЕРИАЛОВ

Фонд оценочных материалов по дисциплине (модулю), состоящий из ФОМ для текущего контроля и проведения промежуточной аттестации обучающихся, разрабатывается по каждой дисциплине. Оценочные материалы размещаются 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	Курило А. П., Милославская Н. Г., Сенаторов М. Ю., Толстой А. И.	Основы управления информационной безопасностью: допущено Учебно-методическим объединением высших учебных заведений России по образованию в области информационной безопасности в качестве учебного пособия для студентов высших учебных заведений, обучающихся по программам бакалавриата, магистратуры и специалитета укрупненного направления 090000 - "Информационная безопасность"	Москва: Горячая линия - Телеком, 2012	
6.1.2. Дополнительная учебная литература				
	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
Л2.1	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	
Л2.2	Шаньгин В.Ф.	Комплексная защита информации в корпоративных системах: Учебное пособие	Москва: Издательский Дом "ФОРУМ", 2020	http://znanium.com
6.1.3. Методические разработки				
	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
Л3.1	Зырянова Т. Ю.	Основы управления информационной безопасностью: методические рекомендации по организации самостоятельной работы студентов по дисциплине «Основы управления информационной безопасностью» для студентов направления подготовки 10.03.01 «Информационная безопасность» очной формы обучения	Екатеринбург: УрГУПС, 2016	http://biblioserver.usurt.ru
Л3.2	Зырянова Т. Ю., Симонович В. Г.	Основы управления информационной безопасностью: методические рекомендации к практическим занятиям по дисциплине «Основы управления информационной безопасностью» для студентов направления подготовки 10.03.01 «Информационная безопасность» очной формы обучения	Екатеринбург: УрГУПС, 2016	http://biblioserver.usurt.ru

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)	
Э1	Интернет портал ISO27000.RU (ЗАЩИТА-ИНФОРМАЦИИ.SU) (http://iso27000.ru)
Э2	Информационный бюллетень компании "Инфосистемы Джет" (http://www.jetinfo.ru)
Э3	Система электронной поддержки обучения Blackboard Learn (http:// bb.usurt.ru)
Э4	Официальный сайт ОАО "российские железные дороги" (http://www.rzd.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	Программное обеспечение компьютерного тестирования АСТ
6.3.1.4	Система электронной поддержки обучения Blackboard Learn
6.3.1.5	Statistica
6.3.1.6	Matlab
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)

6.3.2.4	Банк данных угроз безопасности информации ФСТЭК России: https://bdu.fstec.ru/
6.3.2.5	Государственный реестр сертифицированных средств защиты информации N РОСС RU.0001.01БИ00
6.3.2.6	ГОСТ Эксперт - единая база ГОСТов Российской Федерации

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

Назначение	Оснащение
Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа (практических занятий, лабораторных занятий), курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также для самостоятельной работы. Специализированный кабинет «Управление информационной безопасностью».	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 Технические средства обучения - Комплект мультимедийного оборудования
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
Центр тестирования - Учебная аудитория для проведения текущего контроля и промежуточной аттестации	Специализированная мебель Моноблоки с установленным лицензионным ПО, включая ПО АСТ-Тест, с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Университета
Компьютерный класс - Учебная аудитория для проведения текущего контроля и промежуточной аттестации	Специализированная мебель Компьютерная техника с установленным лицензионным ПО, включая ПО АСТ-Тест, с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Университета
Компьютерный класс - Учебная аудитория для проведения практических (занятий семинарского типа) и лабораторных занятий, групповых и индивидуальных консультаций	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
Читальный зал Информационно-библиотечного центра ИБК УрГУПС - Аудитория для самостоятельной работы	Специализированная мебель Компьютерная техника с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Университета

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.

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).
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)".
При применении дистанционных технологий и электронного обучения освоение дисциплины (модуля) осуществляется в электронно-информационной образовательной среде (образовательная платформа электронной поддержки обучения Blackboard Learn (сайт bb.usurt.ru)) в рамках созданного курса, что позволяет реализовывать асинхронное и синхронное взаимодействие участников образовательных отношений.