МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА
федеральное государственное бюджетное образовательное учреждение высшего образования
САМАРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПУТЕЙ СООБЩЕНИЯ
(СамГУПС)

УТВЕРЖДЕНА:
решением Учёного совета СамГУПС
протокол №50 от 27.03.19г.
в составе основной профессиональной образовательной программы

АКТУАЛИЗИРОВАНА:
решением Учёного совета СамГУПС
протокол Учёного совета СамГУПС №_.№59 от 25.02.20г.

решением Учёного совета СамГУПС
протокол Учёного совета СамГУПС №___от_____.

решением Учёного совета СамГУПС
протокол Учёного совета СамГУПС №___от_____.

Безопасность информационных технологий и систем

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Прикладная математика, информатика и информационные системы**

Учебный план 09.03.02-19-1-ИСТб.plm.plx
09.03.02 Информационные системы и технологии
Информационные системы и технологии на транспорте

Квалификация **бакалавр**

Форма обучения **очная**

Общая трудоемкость **5 ЗЕТ**

Часов по учебному плану 180
в том числе:
аудиторные занятия 72
самостоятельная работа 72
часов на контроль 33,65

Виды контроля в семестрах:
экзамены 6

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр	**6 (3.2)**		Итого	
Недель	17			
Вид занятий	УП	РП	УП	РП
Лекции	36	36	36	36
Лабораторные	18	18	18	18
Практические	18	18	18	18
Контактные часы	2,35	2,35	2,35	2,35
Итого ауд.	72	72	72	72
Контактная	74,35	74,35	74,3	74,35
Сам. работа	72	72	72	72
Часы на контроль	33,65	33,65	33,6	33,65
Итого	180	180	180	180

Самара 2019

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Целью изучения дисциплины "Безопасность информационных технологий и систем" является формирование у обучаемых знаний, умений и навыков (уровня сформированности соответствующих компетенций) в результате последовательного изучения содержательно связанных между собой разделов (тем) учебных занятий, а также подготовить студентов к организации и эксплуатации средств защиты компьютерной информации.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.В.22
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Визуальное программирование
2.1.2	Микропроцессорные информационно-управляющие системы
2.1.3	Надежность информационных систем
2.1.4	Компонентное программирование
2.1.5	Системное программирование
2.1.6	Компьютерные сети и распределенные вычисления
2.1.7	Схемотехника
2.1.8	Безопасность жизнедеятельности
2.1.9	Электротехника и электроника
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Взаимодействие видов транспорта в рамках цифровых технологий
2.2.2	Основы программной инженерии
2.2.3	Эксплуатационное обслуживание информационных систем на железнодорожном транспорте
2.2.4	Производственная практика, преддипломная практика

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)
УК-8: Способен создавать и поддерживать безопасные условия жизнедеятельности, в том числе при возникновении чрезвычайных ситуаций

Индикатор	УК-8.1. Знать: классификацию и источники чрезвычайных ситуаций природного и техногенного происхождения; причины, признаки и последствия опасностей, способы защиты от чрезвычайных ситуаций; принципы организации безопасности труда на предприятии, технические средства защиты людей в условиях чрезвычайной ситуации.
Индикатор	УК-8.2. Уметь: поддерживать безопасные условия жизнедеятельности; выявлять признаки, причины и условия возникновения чрезвычайных ситуаций; оценивать вероятность возникновения потенциальной опасности и принимать меры по ее предупреждению.
Индикатор	УК-8.3. Владеть: методами прогнозирования возникновения опасных или чрезвычайных ситуаций; навыками по применению основных методов защиты в условиях чрезвычайных ситуаций.

ПКР-1: Способность выполнять интеграцию программных модулей и компонент

Индикатор	ПКР-1.1. Знать: методы и средства интеграции модулей и компонент программного обеспечения; интерфейсы взаимодействия модулей системы между собой и с внешней средой; методы и средства разработки процедур развертывания программного обеспечения; методы и средства верификации работоспособности выпусков программной продукции; языки, утилиты и среды программирования, средства пакетного выполнения процедур.
Индикатор	ПКР-1.2. Уметь: Выполнять процедуры сборки программных модулей и компонент в программный продукт. Проводить оценку работоспособности программного продукта; документировать произведенные действия, выявленные проблемы и способы их устранения; производить настройки параметров программного продукта и осуществлять запуск процедур сборки; проводить оценку работоспособности программного продукта; создавать резервные копии программ и данных, выполнять восстановление, обеспечивать целостность программного продукта и данных.
Индикатор	ПКР-1.3. Иметь навыки: интеграции программных компонент собственной разработки и приобретенных; разработки и осуществления процедур верификации выпусков (сборок) программной продукции.

ПКС-2: Способность разрабатывать, эксплуатировать, ремонтировать электронные устройства цифровой автоматики на железной дороге

Индикатор	ПКС-2.1. Знать: принципы проектирования, разработки и эксплуатации устройств цифровой автоматики на железной дороге, включая программируемые с использованием микропроцессоров и микроконтроллеров.
Индикатор	ПКС-2.2. Уметь: разрабатывать устройства цифровой автоматики, осуществлять техническое обслуживание, поиск и устранение неисправностей с применением современных программных и аппаратных инструментов; разрабатывать и применять проектную и эксплуатационную техническую документацию устройств цифровой автоматики.
Индикатор	ПКС-2.3. Иметь навыки: разработки устройств цифровой автоматики, их документирования, поиска и устранения неисправностей с применением современных аппаратных и аппаратных инструментов.

ПКС-3: Способность разрабатывать и модифицировать программное обеспечение, включая написание и отладку программных компонент

Индикатор	ПКС-3.1. Знать: базовые принципы и современные методы алгоритмизации, написания программ и автономной отладки при программировании последовательных, параллельных, распределенных приложений, приложений реального времени; современные языки и средства программирования.
Индикатор	ПКС-3.2. Уметь: осуществлять разработку и формализованное описание алгоритма решения задачи на современных языках программирования и манипулирования данными, разрабатывать и применять процедуры автономной отладки.
Индикатор	ПКС-3.3. Иметь навыки: алгоритмизации, разработки и автономной отладки программных модулей и компонент с использованием современных языков и средств программирования и манипулирования данными при создании последовательных, параллельных, распределенных приложений и приложений реального времени.

В результате освоения дисциплины (модуля) обучающийся должен

3.1	**Знать:**
3.1.1	принципы и методы организации угроз, атак и вторжения; - модели безопасности и секретности.
3.2	**Уметь:**
3.2.1	обнаруживать угрозы, атаки и вторжения, шифровать
3.3	**Владеть:**
3.3.1	программными и техническими средства защиты компьютерной информации.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература	Инте ракт.	Примечание
	Раздел 1. Основные понятия и положения защиты информации в компьютерных системах						
1.1	Введение. Доктрина информационной безопасности России. Основные понятия и определения информационной безопасности. /Лек/	6	2	УК-8	Л1.1Л2.1 Л2.2 Э1	0	
1.2	Понятия экономической и информационной безопасности. Ключевые вопросы ИБ. Экономическая и информационная безопасность. Составляющие информационной безопасности. /Лек/	6	2	ПКС-2	Л1.1Л2.1 Л2.2 Э1	0	
1.3	Предмет и объект защиты. Угрозы безопасности информации в компьютерных системах. /Лек/	6	2	ПКР-1	Л1.1Л2.1 Л2.2 Э1	0	
1.4	Виды угроз информационной безопасности и классификация источников угроз. Основные виды защищаемой информации. /Лек/	6	2	ПКС-2	Л1.1Л2.1 Л2.2 Э1	0	
1.5	Краткий обзор зарубежного законодательства в области информационной безопасности. Российское законодательство в области информационной безопасности. Закон «Об информации, информационных технологиях и защите информации». Другие законы и нормативные акты. /Лек/	6	2	УК-8	Л1.1Л2.1 Л2.2 Э1	0	

1.6	Основы законодательства в области обеспечения информационной безопасности /Пр/	6	2	УК-8	Л1.1Л2.1 Л2.2 Э1	0	
	Раздел 2. Направления обеспечения информационной безопасности.						
2.1	Правовая защита. Организационная защита. Инженерно-техническая защита. /Лек/	6	2	ПКС-2	Л1.2Л2.1 Л2.2	0	
2.2	Программные средства защиты. Криптографические средства защиты. /Лек/	6	2	ПКС-3	Л1.2Л2.1 Л2.2	0	
2.3	Хакерские утилиты и прочие вредоносные программы. Классические компьютерные вирусы. Скрипт-вирусы. Троянские программы. Сетевые черви. /Пр/	6	4	УК-8	Л1.2Л2.1 Л2.2Л3.3 Э2 Э3	0	
2.4	Обеспечение антивирусной защиты операционных систем на основе продуктов компании «Лаборатория Касперского». /Пр/	6	4	ПКР-1	Л1.2Л2.1 Л2.2Л3.3 Э3	0	
2.5	От чего надо защищаться в первую очередь? Как надо защищаться? Антивирусная защита. Современные средства биометрической идентификации. /Пр/	6	4	ПКС-3	Л1.2Л2.1 Л2.2Л3.1 Э3	0	
2.6	Идентификация и аутентификация. Парольная зашита. /Пр/	6	4	ПКС-3	Л1.2Л2.1 Л2.2Л3.1	0	
2.7	Классические методы шифрования. /Лаб/	6	4	ПКР-1	Л1.2Л2.1 Л2.2Л3.3 Э4	0	
2.8	Изучение криптографического стандарта DES /Лаб/	6	4	ПКР-1	Л1.2Л2.1Л3.2 Э4	0	
2.9	Изучение криптографического стандарта ГОСТ 28147-89 /Лаб/	6	4	ПКР-1	Л1.2Л2.1 Л2.2Л3.2 Э4	0	
	Раздел 3. Построения системы информационной безопасности						
3.1	Основные аспекты построения системы информационной безопасности. Программа информационной безопасности. Модели ИБ, требования и основные этапы реализации информационной безопасности. /Лек/	6	2	УК-8	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	
3.2	Мероприятия по защите информации. Политика информационной безопасности. /Лек/	6	2	УК-8	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	
3.3	Анализ и управление рисками при реализации информационной безопасности. Соотношение эффективности и рентабельности систем информационной безопасности. /Лек/	6	2	УК-8	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	
	Раздел 4. Защита информации в информационных системах и компьютерных сетях						
4.1	Определение защищенной информационной системы. Требования к архитектуре ИС для обеспечения безопасности ее функционирования. /Лек/	6	2	ПКС-3	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	

4.2	Методология анализа защищенности информационной системы. Концепция защищенных виртуальных частных сетей. /Лек/	6	2	ПКС-3	Л1.1 Л1.2Л2.1 Л2.2Л3.3 Э1	0	
	Раздел 5. Защита информации от утечки по техническим каналам						
5.1	Способы защиты информации. Характеристика защитных действий. /Лек/	6	2	ПКС-2	Л1.1 Л1.2Л2.1 Л2.2	0	
5.2	Защита информации от утечки по визуально-оптическим каналам. Защита информации от утечки по акустическим каналам. Защита информации от утечки по электромагнитным. Защита информации от утечки по материально-вещественным каналам. /Лек/	6	2	ПКС-2	Л1.1 Л1.2Л2.1 Л2.2	0	
	Раздел 6. Противодействие несанкционированному доступу к источникам конфиденциальной информации						
6.1	Способы несанкционированного доступа. Технические средства несанкционированного доступа к информации. Защита от наблюдения и фотографирования. Защита от подслушивания. /Лек/	6	2	ПКС-2	Л1.1 Л1.2Л2.1 Л2.2	0	
6.2	Защита от копирования. Привязка к аппаратному обеспечению. Использование реестра. /Лек/	6	2	ПКС-3	Л1.1 Л1.2Л2.1 Л2.2	0	
6.3	Защита от копирования. /Лаб/	6	2	УК-8	Л1.1 Л1.2Л2.1 Л2.2Л3.1	0	
6.4	Передача зашифрованных сообщений по электронной почте /Лаб/	6	4	УК-8	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Э4	0	
	Раздел 7. Защита информации в электронных платежных системах						
7.1	Принципы функционирования электронных платежных систем. Электронные пластиковые карты. /Лек/	6	2	УК-8	Л1.1 Л1.2Л2.1 Л2.2 Э5	0	
7.2	Персональный идентификационный номер. Универсальная электронная платежная система UEPS. Обеспечение безопасности электронных платежей через сеть Internet. /Лек/	6	2	УК-8	Л1.1 Л1.2Л2.1 Л2.2 Э5	0	
	Раздел 8. Самостоятельная работа						
8.1	Подготовка к лекциям /Ср/	6	36	УК-8 ПКР-1 ПКС-2 ПКС -3	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э5	0	
8.2	Подготовка к практическим занятиям /Ср/	6	18	УК-8 ПКР-1 ПКС-3	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.3 Э1 Э2 Э3	0	
8.3	Подготовка к лабораторным занятиям /Ср/	6	18	УК-8 ПКР-1	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Л3.3 Э4	0	
	Раздел 9. Контактные часы на аттестацию						

9.1	Аттестация /КЭ/	6	2,35	УК-8 ПКР-1 ПКС-2 ПКС -3	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Л3.3 Э1 Э2 Э3 Э4 Э5	0	

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1. Структура и содержание ФОС

1. Описание показателей и критериев оценивания компетенций
2. Типовые контрольные задания для оценки знаний, умений, навыков и (или) опыта деятельности
3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

5.2. Показатели и критерии оценивания компетенций

Критерии формирования оценок по экзамену
«Отлично» (5 баллов) – обучающийся демонстрирует знание всех разделов изучаемой дисциплины: содержание базовых понятий и фундаментальных проблем; умение излагать программный материал с демонстрацией конкретных примеров. Свободное владение материалом должно характеризоваться логической ясностью и четким видением путей применения полученных знаний в практической деятельности, умением связать материал с другими отраслями знания.
«Хорошо» (4 балла) – обучающийся демонстрирует знания всех разделов изучаемой дисциплины: содержание базовых понятий и фундаментальных проблем; приобрел необходимые умения и навыки, освоил вопросы практического применения полученных знаний, не допустил фактических ошибок при ответе, достаточно последовательно и логично излагает теоретический материал, допуская лишь незначительные нарушения последовательности изложения и некоторые неточности. Таким образом данная оценка выставляется за правильный, но недостаточно полный ответ.
«Удовлетворительно» (3 балла) – обучающийся демонстрирует знание основных разделов программы изучаемого курса: его базовых понятий и фундаментальных проблем. Однако знание основных проблем курса не подкрепляются конкретными практическими примерами, не полностью раскрыта сущность вопросов, ответ недостаточно логичен и не всегда последователен, допущены ошибки и неточности.
«Неудовлетворительно» (0 баллов) – выставляется в том случае, когда обучающийся демонстрирует фрагментарные знания основных разделов программы изучаемого курса: его базовых понятий и фундаментальных проблем. У экзаменуемого слабо выражена способность к самостоятельному аналитическому мышлению, имеются затруднения в изложении материала, отсутствуют необходимые умения и навыки, допущены грубые ошибки и незнание терминологии, отказ отвечать на дополнительные вопросы, знание которых необходимо для получения положительной оценки.

5.3. Типовые контрольные задания для оценки знаний, умений, навыков и (или) опыта деятельности

5.4. Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Описание процедуры оценивания «Дискуссия». Дискуссия может быть организована как в ходе проведения лекционного, так и в ходе практического занятия. Для эффективного хода дискуссии обучающиеся могут быть поделены на группы, отстаивающие разные позиции по одному вопросу. Преподаватель контролирует течение дискуссии, помогает обучающимся подвести её итог, сформулировать основные выводы и оценивает вклад каждого участника дискуссии в соответствии с критериями, описанными в пункте 5.2.
Оценивание итогов практической работы проводится преподавателем, ведущим практические занятия и лабораторные работы.
По результатам проверки отчета по практической работе и по работе в малых группах обучающийся допускается к его защите при условии соблюдения перечисленных условий:
– выполнены все задания;
– отсутствуют ошибки;
– оформлено в соответствии с требованиями.
В том случае, если содержание отчета не отвечает предъявляемым требованиям, то он возвращается автору на доработку. Обучающийся должен переделать отчет с учетом замечаний. Если сомнения вызывают отдельные аспекты отчета, то в этом случае они рассматриваются во время устной защиты.
Защита отчета по практической работе и по работе в малых группах представляет собой устный публичный отчет обучающегося о результатах выполнения задания, ответы на вопросы преподавателя.
Ответ обучающегося оценивается преподавателем в соответствии с критериями, описанными в пункте 5.2.
При проведении экзамена в форме тестирования в системе «Moodle» (режим доступа: http://do.samgups.ru/moodle/) количество тестовых заданий и время задается системой. Результат каждого обучающегося оценивается в соответствии с универсальной шкалой, приведенной в пункте 5.2.

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

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Кол-во	Издательс	Эл. адрес

	Авторы, составители	Заглавие	Кол-во	Издательс	Эл. адрес
Л1.1	Корниенко А. А.	Информационная безопасность и защита информации на железнодорожном транспорте. В 2 ч. Ч. 1. Методология и система обеспечения информационной безопасности на железнодорожном транспорте: учебник для вузов	45	Москва: УМЦ по образован ию на железнодо рожном транспорт е, 2014	
Л1.2	Корниенко А. А.	Информационная безопасность и защита информации на железнодорожном транспорте. В 2 ч. Ч. 2. Программно-аппаратные средства обеспечения информационной безопасности на железнодорожном транспорте: учебник для вузов	45	Москва: УМЦ по образован ию на железнодо рожном транспорт е, 2014	

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Кол-во	Издательс	Эл. адрес
Л2.1	Бурова М. А., Овсянников А. С.	Информационная безопасность и защита информации: конспект лекций	1 Электро нное издание	Самара: СамГУПС , 2012	ftp://172.16. 0.70/Lekzii/
Л2.2	Корниенко А.А., Еремеев М.А., Кустов В.Н., Иванов Д.Д., Горелик В.Ю.	Информационная безопасность и защита информации на железнодорожном транспорте. Часть 2: учебник: в 2 ч.	1 Электро нное издание	Москва: ФГБОУ «Учебно-методичес кий центр по образован ию на железнодо рожном транспорт е», 2015	https://umcz dt.ru/books/4 2/30051/

6.1.3. Методические разработки

	Авторы, составители	Заглавие	Кол-во	Издательс	Эл. адрес
Л3.1	Часовских Е. А., Сундуков М. В., Чигринский Р. И.	Аппаратные и программные средства защиты информации: метод. указ. к вып. лаб. работ по дисц. Безопасность информ. систем для магистров по напр. подгот. 230400 Информ. системы и технологии	1 Электро нное издание	Самара: СамГУПС , 2013	http://do.sam gups.ru/moo dle/course/vi ew.php? id=4070
Л3.2	Тюмиков Д. К.	Криптографические методы обеспечения информационной безопасности и защиты информации: метод. указ. к вып. лаб. работ для магистров по напр. подгот. 220100.68 САУ	20	Самара: СамГУПС , 2014	
Л3.3	Тюмиков Д. К.	Инструментальные средства защиты информации в WINDOWS: метод. указ. к вып. лаб. работ для бакалавров по напр. подгот. 220100.62 САУ по дисц. Методы и средства защиты компьютерной информ.	22	Самара: СамГУПС , 2014	

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	Граничин Олег, Кияев Владимир Безопасность информационных систем. [Электронный ресурс]: курс дистанц. обучения / НОЧУ ДПО «Национальный Открытый Университет «ИНТУИТ»» URL: https://www.intuit.ru/studies/courses/13845/1242/info (дата обращения: 21. 01. 2020).
Э2	Вирусы и средства борьбы с ними. [Электронный ресурс]: курс дистанц. обучения / НОЧУ ДПО «Национальный Открытый Университет «ИНТУИТ»» URL: https://www.intuit.ru/studies/courses/1042/154/info. (дата обращения: 21. 01. 2020).
Э3	Антивирусная защита компьютерных систем. [Электронный ресурс]: курс дистанц. обучения / НОЧУ ДПО «Национальный Открытый Университет «ИНТУИТ»» URL: https://www.intuit.ru/studies/courses/2259/155/info. (дата обращения: 21. 01. 2020).
Э4	Жданов Олег, Ушаков Юрий. Криптографические методы защиты информации. [Электронный ресурс]: курс дистанц. обучения / НОЧУ ДПО «Национальный Открытый Университет «ИНТУИТ»» URL: https://www.intuit.ru/studies/courses/13837/1234/info. (дата обращения: 21. 01. 2020).

Э5	Иванов Михаил, Михайлов Дмитрий, Чугунков Илья. Защита информации в электронных платежных системах. [Электронный ресурс]: курс дистанц. обучения / НОЧУ ДПО «Национальный Открытый Университет «ИНТУИТ»» URL: https://www.intuit.ru/studies/courses/3580/822/info. (дата обращения: 21. 01. 2020).

6.3 Информационные технологии, используемые при осуществлении образовательного процесса по дисциплине (модулю)

6.3.1 Перечень программного обеспечения

6.3.1.1	Windows 2003 Server, Windows 7, Windows 8, Microsoft Office 2013, Microsoft Visual Studio® 2013, Code Blocks, Lazarus 1.4.0 (аналог Delphi), Libre Office 4.3 (аналог MS Office), Dia (аналог All FusionProcess Modeller), Microsoft SQL Server® 2008 R2 Developer, Enterprise, and Standard Edition, Microsoft SQL Server® 2012, Java, Virtual Box, Scilab 5.4.1 (аналог Matlab).

6.3.2 Перечень профессиональных баз данных и информационных справочных систем

6.3.2.1	www.apps.webofknowledge.com - Наукометрическая реферативная база данных журналов и конференций.
6.3.2.2	www.scopus.com - крупнейшая единая база данных, содержащая аннотации и информацию о цитируемости рецензируемой научной литературы.
6.3.2.3	www.clarivate.ru - база данных авторитетных российских журналов.
6.3.2.4	www.elibrary.ru - Крупнейший российский информационный портал в области науки, технологии, медицины и образования Доступ свободный.
6.3.2.5	www.garant.ru - Система «ГАРАНТ»
6.3.2.6	www.consultant.ru - система «КонсультантПлюс».
6.3.2.7	www.e.lanbook.com - Электронно-библиотечная система Издательства Лань.
6.3.2.8	www.biblio-online.ru - Электронная библиотечная система «Юрайт».

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1	Аудитории для проведения лекционных, лабораторных и практических занятий (25 и более посадочных мест) оборудованные учебной доской, партами, стульями; неограниченный доступ к электронно-библиотечным системам (через ресурсы библиотеки СамГУПС), к электронной информационно-образовательной среде moodle и к информационно-телекоммуникационной сети «Интернет» в рамках самостоятельной работы обучающегося. Проведение занятий должно осуществляться с помощью современных мультимедийных интерактивных обучающих систем, что требует оборудования учебных аудиторий соответствующими техническими и программными средствами. Лабораторные и практические занятия должны проводиться в специализированных аудиториях кафедры ПМИИС: 1206 лаборатория «Сети ЭВМ и информационные системы», 1309 лаборатория «Информационно-измерительные и управляющие системы», 1310 лаборатория «Имитационное моделирование систем и процессов» и 1308 лаборатория «НИР бакалавров, магистров и аспирантов». Кабинет выполнения курсовых и выпускных квалификационных работ.

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

Для освоения дисциплины обучающемуся необходимо: систематически посещать лекционные занятия; активно участвовать в обсуждении предложенных вопросов и выполнять задания практических занятий и задания по работе в малых группах; написать и провести защиту курсовой работы, успешно пройти все формы текущего контроля; сдать экзамен (вопросы прилагаются).
Для подготовки к итоговым испытаниям по дисциплине необходимо использовать: материалы лекций, рекомендуемой основной и дополнительной литературы; методические материалы (практикумы и МУ).
Для теоретического и практического усвоения дисциплины большое значение имеет самостоятельная работа обучающихся, которая может осуществляться как индивидуально, так и под руководством преподавателя. Данная работа предполагает самостоятельное изучение обучающимся отдельных тем, дополнительную подготовку к каждому лекционному, лабораторному и практическому