ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

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

Б1.В.02 Информационная безопасность объектов транспортной инфраструктуры

рабочая программа дисциплины (модуля)

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

Учебный план 10.04.01_ИБм_2021.plx
Направление подготовки 10.04.01 Информационная безопасность

Направленность (профиль) Информационная безопасность на транспорте

Квалификация **магистр**

Форма обучения **очная**

Объем дисциплины (модуля) **5 ЗЕТ**

Часов по учебному плану 180
в том числе:
аудиторные занятия 48
самостоятельная работа 60
часов на контроль 36

Промежуточная аттестация и формы контроля:
экзамен 3

Часов контактной работы всего, в том числе: 54,1
аудиторная работа 48
текущие консультации по лабораторным занятиям 1,2
текущие консультации по практическим занятиям 2,4
консультации перед экзаменом 2
прием экзамена 0,5

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**3 (2.1)**		Итого	
Недель	12			
Вид занятий	УП	РП	УП	РП
Лекции	12	12	12	12
Лабораторные	12	12	12	12
Практические	24	24	24	24
Элект	36	36	36	36
Итого ауд.	48	48	48	48
Контактная работа	84	84	84	84
Сам. работа	60	60	60	60
Часы на контроль	36	36	36	36
Итого	180	180	180	180

1. ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Цель дисциплины: изучение правовых, организационных и технических механизмов построения систем обеспечения информационной безопасности значимых объектов транспортной инфраструктуры.
1.2	Задачи дисциплины: изучение основных понятий, методологии и практических приемов управления технической и организационной инфраструктурой обеспечения информационной безопасности на предприятии; приобретение обучаемыми необходимого объема знаний и практических навыков в области управления информационной безопасностью в системах критической информационной инфраструктуры; 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.В

2.1 Требования к предварительной подготовке обучающегося:

Для изучения данной учебной дисциплины необходимы знания, умения и навыки, приобретенные в ходе освоения программ бакалавриата и/или специалитета и дисциплин Управление информационной безопасностью, Технологии обеспечения информационной безопасности.
В результате освоения предшествующих дисциплин обучающийся должен знать: принципы организации защиты информации; подходы к построению модели нарушителя и объекта с точки зрения информационной безопасности; уметь: обосновать принципы организаци технического, программного и информационного обеспечения информационной безопасности; владеть: навыками работы с нормативными правовыми актами; навыками работы с нормативными документами; методами и средствами выявления угроз безопасности автоматизированным системам.

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

Производственная практика (преддипломная практика)
Государственная итоговая аттестация

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ
ПК-1: Способен разрабатывать требования по защите, формировать политики безопасности компьютерных систем и сетей
ПК-1.3: Определяет угрозы безопасности информации, реализация которых может привести к нарушению безопасности информации в компьютерной системе и сети и разрабатывает модель угроз безопасности информации
ПК-1.2: Классифицирует информационную систему по требованиям защиты информации
ПК-1.1: Знает модели безопасности и виды политик безопасности компьютерных систем и сетей
ПК-2: Способен проводить анализ безопасности компьютерных систем
ПК-2.3: Анализирует компьютерную систему с целью определения уровня защищенности и доверия
ПК-2.4: Прогнозирует возможные пути развития действий нарушителя информационной безопасности
ПК-2.1: Знает национальные, межгосударственные и международные стандарты в области защиты информации, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации
ПК-2.2: Оценивает риски, связанные с осуществлением угроз безопасности в отношении компьютерных систем
ПК-3: Способен участвовать в проведении аттестации объектов вычислительной техники на соответствие требованиям по защите информации
ПК-3.3: Применяет технические средства защиты информации от утечки за счет побочных электромагнитных излучений и наводок
ПК-3.2: Знает способы защиты информации от утечки за счет побочных электромагнитных излучений и наводок
ПК-3.1: Знает технические каналы утечки информации, возникающие за счет побочных электромагнитных излучений и наводок
ПК-4: Способен участвовать в проведении аттестации выделенных (защищаемых) помещений на соответствие требованиям по защите информации
ПК-4.3: Применяет технические средства защиты акустической речевой информации от утечки по техническим каналам
ПК-4.2: Знает способы защиты акустической речевой информации от утечки по техническим каналам
ПК-4.1: Знает технические каналы утечки акустической речевой информации
ПК-6: Моделирует и исследует технологии автоматизации информационно-аналитической деятельности, осуществляет информационно-аналитическую поддержку процессов принятия решений

ПК-6.2: Разрабатывает и исследует формализованные модели автоматизированных технологий анализа информации

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	правовые, организационные и технические основы обеспечения безопасности значимых объектов транспортной инфраструктуры; модели безопасности компьютерных систем и сетей; национальные и международные стандарты, руководящие документы органов исполнительной власти по защите информации; основные технические каналы утечки информации и способы их блокирования
3.2	**Уметь:**
3.2.1	определять угрозы безопасности информации; оценивать риски, связанные с осуществлением угробз безопасности информации; применять организационные меры и технические средства защиты информации на значимых объектах транспортной инфраструктуры;
3.2.2	использовать существующие и разрабатывать новые модели угроз и модели нарушителя безопасности информационных систем
3.3	**Владеть:**
3.3.1	способами анализа защищенности информационных систем с использованием моделей безопасности; навыками разработки системы безопасности объекта транспортной инфраструктуры; навыками применения требований по аттестации объектов информатизации на соответствие требованиям по защите информации

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов (академических)	Компетенции	Литература	Активные формы
	Раздел 1. Основы обеспечения информационной безопасности объектов транспортной инфраструктуры					
1.1	Правовые основы обеспечения безопасности /Лек/	3	1	ПК-2.1	Л1.1 Л1.2 Э1 Э2 Э3 Э4	
1.2	Объекты защиты, основные понятия, цели и задачи обеспечения информационной безопасности /Лек/	3	1	ПК-2.1	Л1.1 Л1.2 Э1 Э2 Э3 Э4	
1.3	Система сертификации по требованиям безопасности информации /Лек/	3	2	ПК-2.1	Л1.1 Л1.2 Э1 Э2 Э3 Э4	
1.4	Основополагающие принципы обеспечения безопасности объектов транспортной инфраструктуры /Лек/	3	2	ПК-2.1	Л1.1 Л1.2 Э1 Э2 Э3 Э4	
1.5	Правовое регулирование вопросов обеспечения безопасности в отношении различных объектов транспортной инфраструктуры /Пр/	3	2	ПК-2.1	Л1.1 Л1.2Л3.1 Э1 Э2 Э3 Э4	Работа в группах, анализ нормативных, правовых и методических документов
1.6	Субъекты информационных отношений, права, обязанности, особенности взаимодействия /Пр/	3	2	ПК-2.1	Л1.1 Л1.2Л3.1 Э1 Э2 Э3 Э4	Работа в группах, анализ нормативных, правовых и методических документов
1.7	Основные понятия в области траноспортной безопасности /Пр/	3	2	ПК-2.1	Л1.1 Л1.2Л3.1 Э1 Э2 Э3 Э4	Работа в группах, анализ нормативных, правовых и методических документов
1.8	Организационные основы противодействия терроризму /Пр/	3	2	ПК-2.1 ПК-2.4	Л1.1 Л1.2Л2.2Л3.1 Э1 Э2 Э3 Э4	Работа в группах, анализ нормативных, правовых и методических документов

1.9	Определение актуальных угроз безопасности информации /Пр/	3	2	ПК-1.3 ПК-2.2 ПК-2.3 ПК-2.4	Л1.1 Л1.2Л3.1 Э1 Э2 Э3 Э4	Работа в группах, анализ нормативных, правовых и методических документов
1.10	Формирование перечня объектов, подлежащих защите /Пр/	3	2	ПК-1.2 ПК-1.3 ПК-2.2 ПК-2.3 ПК-2.4	Л1.1 Л1.2Л3.1 Э1 Э2 Э3 Э4	Работа в группах, анализ нормативных, правовых и методических документов
1.11	Работа с реестрами, банком данных угроз безопасности информации /Лаб/	3	12	ПК-1.3 ПК-2.2 ПК-2.4	Л1.1 Л1.2Л3.3 Э1 Э2 Э3 Э4	Работа в малых группах, анализ профессиональных баз данных
1.12	Изучение требований нормативных правовых актов и методических документов в области обеспечения безопасности объектов транспортной инфраструктуры /Ср/	3	10	ПК-1.2 ПК-1.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4	Л1.1 Л1.2Л3.3 Э1 Э2 Э3 Э4	
1.13	Подготовка к практическим семинарам и лабораторным занятиям /Ср/	3	10	ПК-1.1 ПК-1.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4	Л1.1 Л1.2Л3.3 Э1 Э2 Э3 Э4	
1.14	Подготовка доклада на практическом семинаре /Ср/	3	10	ПК-1.1 ПК-1.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4	Л1.1 Л1.2Л3.3 Э1 Э2 Э3 Э4	
	Раздел 2. Организация работ по обеспечению безопасности значимых объектов транспортной инфрастукруры					
2.1	Порядок определения принадлежности организации к критической информационной инфраструктуре /Лек/	3	1	ПК-1.1 ПК-1.2 ПК-2.1 ПК-2.3	Л1.1 Л1.2Л2.1 Л2.2Л3.4 Э1 Э2 Э3 Э4	
2.2	Формирование полного перечня объктов критической информационной инфраструктуры /Лек/	3	1	ПК-1.1 ПК-1.2 ПК-2.1 ПК-2.3	Л1.1 Л1.2Л2.1 Л2.2Л3.4 Э1 Э2 Э3 Э4	
2.3	Категорирование объектов критической информационной инфраструктуры /Лек/	3	1	ПК-1.1 ПК-1.2 ПК-2.1 ПК-2.3	Л1.1 Л1.2Л2.1 Л2.2Л3.4 Э1 Э2 Э3 Э4	
2.4	Построение системы безопасности объектов критичекой информационной инфраструктуры /Лек/	3	2	ПК-3.1 ПК-3.2 ПК-3.3 ПК-4.1 ПК-4.2 ПК-4.3 ПК-6.2	Л1.1 Л1.2Л2.1 Л2.2Л3.4 Э1 Э2 Э3 Э4	
2.5	Выстраивание взаимодействия с Государственной системой обнаружения и противодействия компьютерным атакам /Лек/	3	1	ПК-2.1 ПК-6.2	Л1.1 Л1.2Л2.1 Л2.2Л3.4 Э1 Э2 Э3 Э4	
2.6	Выбор субъекта критической информационной инфраструктуры, определение принадлежности к субъектам критической информационной инфраструктуры по прямому или косвенному методам /Пр/	3	2	ПК-1.2	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.4 Э1 Э2 Э3 Э4	Работа в группах, разработка системы защиты информации
2.7	Формирование отчета об обследовании и полного перечня объектов критической информационной инфраструктуры /Пр/	3	2	ПК-1.2	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.4 Э1 Э2 Э3 Э4	Работа в группах, разработка системы защиты информации

2.8	Формирование перечня объектов критической информационной инфраструктуры в соответствии с установленными требованиями /Пр/	3	2	ПК-1.2	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.4 Э1 Э2 Э3 Э4	Работа в группах, разработка системы защиты информации
2.9	Формирование требований и реализация мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры /Пр/	3	2	ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4 ПК-3.1 ПК-3.2 ПК-3.3 ПК-4.1 ПК-4.2 ПК-4.3	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.4 Э1 Э2 Э3 Э4	Работа в группах, разработка системы защиты информации
2.10	Расчет ущерба (масштаб возможных последствий от реализации компьютерной атаки на информационные системы, обслуживающие критические процессы организации) /Пр/	3	2	ПК-2.2 ПК-6.2	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.4 Э1 Э2 Э3 Э4	Работа в группах, разработка системы защиты информации
2.11	Разработка технического задания на создание системы безопасности объекта транспортной инфраструктуры /Пр/	3	2	ПК-1.1 ПК-1.2 ПК-1.3 ПК-2.1	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.4 Э1 Э2 Э3 Э4	Работа в группах, разработка системы защиты информации
2.12	Изучение нормативных правовых и методических документов в области транспортной безопасности /Ср/	3	10	ПК-1.1 ПК-1.2 ПК-1.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4 ПК-3.1 ПК-3.2 ПК-3.3 ПК-4.1 ПК-4.2 ПК-4.3 ПК-6.2	Л1.1 Л1.2Л2.1 Л2.2Л3.2 Л3.4 Э1 Э2 Э3 Э4	
2.13	Подготовка к практическим семинарам /Ср/	3	10	ПК-1.1 ПК-1.2 ПК-1.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4 ПК-3.1 ПК-3.2 ПК-3.3 ПК-4.1 ПК-4.2 ПК-4.3 ПК-6.2	Л1.1 Л1.2Л2.1 Л2.2Л3.2 Л3.4 Э1 Э2 Э3 Э4	
2.14	Подготовка доклада на практическом семинаре. Подготовка к промежуточной аттестации /Ср/	3	10	ПК-1.1 ПК-1.2 ПК-1.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4 ПК-3.1 ПК-3.2 ПК-3.3 ПК-4.1 ПК-4.2 ПК-4.3 ПК-6.2	Л1.1 Л1.2Л2.1 Л2.2Л3.2 Л3.4 Э1 Э2 Э3 Э4	
2.15	Взаимодействие с обучающимися по вопросам текущего контроля в электронной информационно-образовательной среде: выполнение контрольных заданий и промежуточных тестов по практическим и лабораторным занятиям /Элект/	3	36	ПК-1.1 ПК-1.2 ПК-1.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4 ПК-3.1 ПК-3.2 ПК-3.3 ПК-4.1 ПК-4.2 ПК-4.3 ПК-6.2	Л1.1 Л1.2Л2.1 Л2.2Л3.2 Л3.4 Э1 Э2 Э3 Э4	

2.16	Промежуточная аттестация /Экзамен/	3	36	ПК-1.1 ПК-1.2 ПК-1.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4 ПК-3.1 ПК-3.2 ПК-3.3 ПК-4.1 ПК-4.2 ПК-4.3 ПК-6.2	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Л3.3 Л3.4 Э1 Э2 Э3 Э4	

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	Зырянова Т. Ю.	Информационная безопасность объектов транспортной инфраструктуры: конспект лекций для студентов направления подготовки магистратуры 10.04.01 «Информационная безопасность»	Екатеринбург: УрГУПС, 2016	http://biblioserver.usurt.ru
Л1.2	Ададуров С. Е., Глухов А. П., Иванов Д. Д., Горелик В. Ю.	Информационная безопасность и защита информации на железнодорожном транспорте. Часть 1: учебник: в 2 ч.	Москва: ФГБОУ «Учебно-методический центр по образованию на железнодорожном транспорте», 2015	https://umczdt.ru/books/

6.1.2. Дополнительная учебная литература

	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
Л2.1	Ялышев Ю. И., Миловидов С. Н.	Разработка планов обеспечения транспортной безопасности для объектов транспортной инфраструктуры на железнодорожном транспорте: методические рекомендации	Екатеринбург: УрГУПС, 2014	http://biblioserver.usurt.ru
Л2.2	Васильев И. Л., Миловидов С. Н.	Разработка порядка реагирования сил транспортной безопасности и персонала объекта транспортной инфраструктуры и/или транспортных средств железнодорожного транспорта на угрозы подготовки, совершения актов незаконного вмешательства: методическое пособие	Екатеринбург: УрГУПС, 2014	http://biblioserver.usurt.ru

6.1.3. Методические разработки

	Авторы, составители	Заглавие	Издательство, год	Web-ссылка

	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
Л3.1	Зырянова Т. Ю.	Информационная безопасность объектов транспортной инфраструктуры: методические рекомендации к практическим семинарам по дисциплине «Информационная безопасность объектов транспортной инфраструктуры» для студентов направления подготовки 10.04.01 «Информационная безопасность» очной формы обучения	Екатеринбург: УрГУПС, 2016	http://biblioserver.usurt.ru
Л3.2	Зырянова Т. Ю.	Информационная безопасность объектов транспортной инфраструктуры: методические рекомендации по организации самостоятельной работы по дисциплине «Информационная безопасность объектов транспортной инфраструктуры» для студентов направления подготовки 10.04.01 «Информационная безопасность» очной формы обучения	Екатеринбург: УрГУПС, 2016	http://biblioserver.usurt.ru
Л3.3	Зырянова Т. Ю.	Информационная безопасность объектов транспортной инфраструктуры: методические указания к лабораторным работам для студентов направления подготовки магистратуры 10.04.01 «Информационная безопасность»	Екатеринбург: УрГУПС, 2016	http://biblioserver.usurt.ru
Л3.4	Горнева О. С.	Объекты транспортной инфраструктуры: практикум для обучающихся по направлению подготовки 38.03.01 «Экономика», профиль «Экономика строительного бизнеса» всех форм обучения	Екатеринбург: УрГУПС, 2021	http://biblioserver.usurt.ru

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

Э1	Официальный сайт Министурства транспорта Российской Федерации (http://www.mintrans.ru)
Э2	Официальный сайт ФСТЭК России (http://www.fstec.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	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	ГОСТ Эксперт - единая база ГОСТов Российской Федерации
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	ЭБС УМЦ ЖДТ по адресу https://umczdt.ru/books/
6.3.2.7	ЭБС IPR SMART по адресу http://www.iprbookshop.ru/586.html

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

Назначение	Оснащение
Лаборатория «Программно-аппаратные средства защищенных информационных систем». Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа	Специализированная мебель Лабораторное оборудование: Аппаратно-программный комплекс шифрования "Континент" Программно-аппаратный комплекс защиты информации ViPNet Custom, включающий в том числе киптографические средства" Оборудование для центра защиты информации, включающее в том числе интегрированную систему безопасности "Рубеж", видеоохранную систему видеонаблюдения "Купол", аппартные средства аутетификации пользователя

(практических занятий, лабораторных занятий), курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	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
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
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
Лаборатория «Технологии обеспечения информационной безопасности и техническая защита информации». 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.	Специализированная мебель Лабораторное оборудование: Анализатор качества электроэнергии в трехфазных сетях FLUKE 435 Анализатор спектра портативный R&S FSH 4/8 Комплекс программно-аппаратный Oscor-5000 Всенаправленный источник звука Bruel&Kjaer 4296 Генаратор шума "ГРОМ-ЗИ-4" Детектор звукозаписывающих устройств Имитатор электростатических разрядов ЭСР-8000 К Идикатор поля D-008 Подавитель сотовой связи ЛПШ-718 Тестер кабельный MicroScanner2 Универсальный анализатор проводных линий ULAN-2 Шумомер-виброметр, анализатор спектра портативный ОКТАВА-110А с антеннами измерительными Система автоматизированная измерения действующих высот случайных антенн и коэффициентов реального затухания электромагнитных сигналов СТЕНТОР-М1 Комплекс для проведения акустических и виброакустических измерений "Спрут-7А" Оборудование для центра защиты информации, включающее комплекс виброакустической защиты "Барон", поисковый прибор "ОРИОН", измеритель параметров проводных коммуникаций LBD-50, прибор блокирования сотовых телефонов "Скат" Многофункциональный поисковый прибор SPYDER Ручной селективный металлодетектор EH-MD1 Селективный индикатор поля RAKSA-120 Портативный измеритель частоты и мощности РИЧ-8 (MFP-8000) Обнаружитель скрытых видеокамер по оптическому признаку с лазерной подсветкой Прометей Устройство для защиты линий электропитания и заземления от утечки информации. Средство активной защиты информации от утечки за счет ПЭМИН Соната-Р3 Устройство блокирования работы систем цифровой связи и передачи данных Квартет-2 Подавитель диктофонов и микрофонов Бубен-Ультра

	Генератор звуковой акустической помехи Бубен Система активной защиты информации от утечки за счет ПЭМИН SEL SP-44 Однофазный сетевой помехоподавляющий фильтр ЛППФ-10-1Ф Устройство защиты громкоговорителя МП-5 Тестер блокираторов сотовой связи и беспроводной передачи данных
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

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.
Обучающемуся 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 обучающихся 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.
Для закрепления теоретического материала в системе электронной поддержки обучения Blackboard Learn (сайт bb.usurt.ru) размещены тестовые материалы. Число тренировочных попыток ограничено. Тестовые материалы сформированы в логической последовательности в соответствии с изученными темами. Самостоятельная работа организована таким образом, чтобы обучающиеся имели возможность получать обратную связь о ее результатах до начала промежуточной аттестации. Совместная деятельность преподавателя и обучающихся организована в системе электронной поддержки обучения Blackboard Learn (сайт bb.usurt.ru). Для корректной работы в системе обучающиеся в разделе "Личные сведения" должны ввести актуальный адрес своей электронной почты.
Формы самостоятельной работы обучающихся по данной дисциплине разнообразны. Они включают в себя:
- изучение теоретического материала (учебной, научной, методической литературы, материалов периодических изданий);
- подготовку к занятиям, предусмотренным РПД, мероприятиям текущего контроля, промежуточной аттестации и т.д.
Выполнять самостоятельную работу и отчитываться по ее результатам обучающийся должен в соответствии с календарным планом изучения дисциплины, видами и сроками отчетности.
При выполнении самостоятельной работы обучающемуся рекомендуется руководствоваться учебно-методическими материалами, размещенными на странице данного курса в системе электронной поддержки обучения Blackboard Learn (сайт bb.usurt.ru), а также учебно-методическими материалами, которые указаны для самостоятельной работы по темам дисциплины в разделе 4 РПД "Структура и содержание дисциплины (модуля)".
Перечень учебно-методических материалов (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).
При применении дистанционных образовательных 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