

## **Б1.Б.17 Организационное и правовое обеспечение информационной безопасности**

### **рабочая программа дисциплины (модуля)**

Закреплена за кафедрой	<b>Информационные технологии и защита информации</b>		
Учебный план	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)		
<b>Квалификация</b>	<b>Бакалавр</b>		
Форма обучения	<b>очная</b>		
Объем дисциплины (модуля)	<b>5 ЗЕТ</b>		
Часов по учебному плану	180	Часов контактной работы всего, в том числе:	41,3
в том числе:		аудиторная работа	36
аудиторные занятия	36	текущие консультации по практическим занятиям	1,8
самостоятельная работа	108	консультации перед экзаменом	2
часов на контроль	36	прием экзамена	0,5
Промежуточная аттестация и формы контроля:		проверка, защита курсовой работы	1
экзамен 5 КР 5			

#### **Распределение часов дисциплины по семестрам**

Семестр (<Курс>.<Семестр на курсе>)	5 (3.1)		Итого	
	Неделя			
	18			
Вид занятий	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
в том числе КР	36	36	36	36
Часы на контроль	36	36	36	36
<b>Итого</b>	<b>180</b>	<b>180</b>	<b>180</b>	<b>180</b>

<b>1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)</b>	
1.1	Формирование у обучающихся четкого представления о роли информационной безопасности в становлении и развитии информационного общества.
1.2	Воспитание правовой культуры в области информационной безопасности. Обеспечение изучения обучающимися основных теоретических концепций и базы правовых нормативных актов, регулирующих информационную безопасность.

## **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 дисциплин Правовые и экономические аспекты профессиональной деятельности, 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;  
 владеть: навыками работы с нормативными правовыми актами и основными понятиями, терминологией в области информационной безопасности.

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

Комплексные системы защиты информации на транспорте  
 Защита информационных процессов на транспорте  
 Управление информационной безопасностью на объектах транспортной инфраструктуры  
 Учебная практика (практика по получению первичных профессиональных умений и навыков)  
 Учебная практика (ознакомительная практика)  
 Учебная практика (технологическая практика)  
 Производственная практика (проектно-технологическая практика)  
 Производственная практика (эксплуатационная практика)  
 Преддипломная практика  
 Комплексные системы защиты информации на транспорте

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

**ОПК-5: способностью использовать нормативные правовые акты в профессиональной деятельности**

**Знать:**

Уровень 1	основы российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации; основы организационного и правового обеспечения информационной безопасности
Уровень 2	основы российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации; основы организационного и правового обеспечения информационной безопасности; нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации
Уровень 3	основы российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации; основы организационного и правового обеспечения информационной безопасности; нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации; организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области защиты информации

**Уметь:**

Уровень 1	использовать в практической деятельности правовые знания; анализировать и составлять правовые акты и осуществлять правовую оценку информации; предпринимать необходимые меры по восстановлению нарушенных прав
Уровень 2	использовать в практической деятельности правовые знания; анализировать и составлять правовые акты и осуществлять правовую оценку информации; предпринимать необходимые меры по восстановлению нарушенных прав; применять нормативные правовые акты и нормативные методические документы в области информационной безопасности
Уровень 3	использовать в практической деятельности правовые знания; анализировать и составлять правовые акты и осуществлять правовую оценку информации; предпринимать необходимые меры по восстановлению нарушенных прав; применять нормативные правовые акты и нормативные методические документы в области информационной безопасности; разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации

**Владеть:**

Уровень 1	навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности; навыками работы с нормативными правовыми актами; навыками организации обеспечения режима секретности
Уровень 2	навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности; навыками работы с нормативными правовыми актами; навыками организации обеспечения режима

	секретности; методами организации и управления деятельностью служб защиты информации на предприятии
Уровень 3	навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности; навыками работы с нормативными правовыми актами; навыками организации обеспечения режима секретности; методами организации и управления деятельностью служб защиты информации на предприятии; методами формирования требований по защите информации

**ПК-5: способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации**

<b>Знать:</b>	
Уровень 1	цели, задачи, принципы и основные направления обеспечения информационной безопасности государства; основные термины по проблематике информационной безопасности; методологию создания систем защиты информации
Уровень 2	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 3	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; особенности обеспечения информационной безопасности компьютерных систем при обработке информации, составляющей государственную тайну
<b>Уметь:</b>	
Уровень 1	пользоваться современной научно-технической информацией по исследуемым проблемам и задачам
Уровень 2	пользоваться современной научно-технической информацией по исследуемым проблемам и задачам; определять комплекс мер для обеспечения информационной безопасности
Уровень 3	пользоваться современной научно-технической информацией по исследуемым проблемам и задачам; определять комплекс мер для обеспечения информационной безопасности; организовать проведение и сопровождение аттестации объекта на соответствие требованиям государственных предприятий и корпоративных в том числе
<b>Владеть:</b>	
Уровень 1	навыками формальной постановки и решения задачи обеспечения информационной безопасности информации
Уровень 2	навыками формальной постановки и решения задачи обеспечения информационной безопасности информации; навыками анализа информационной инфраструктуры информационной системы и ее безопасности
Уровень 3	навыками формальной постановки и решения задачи обеспечения информационной безопасности информации; навыками анализа информационной инфраструктуры информационной системы и ее безопасности; навыками участия в экспертизе состояния защищенности информации на объекте защиты

**ПК-9: способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности**

<b>Знать:</b>	
Уровень 1	основные принципы построения комплексных систем защиты информации на предприятии
Уровень 2	основные угрозы информационной безопасности предприятий в различных сферах деятельности
Уровень 3	принципы формирования и реализации политики безопасности в информационных системах предприятий различных сфер деятельности
<b>Уметь:</b>	
Уровень 1	определять информационную инфраструктуру и информационные ресурсы предприятия, подлежащие защите
Уровень 2	разрабатывать модели угроз и модели нарушителей информационной безопасности информационных систем предприятий различных сфер деятельности
Уровень 3	определять комплекс мер (правила, процедуры, практические приемы, руководящие методы, средства) для обеспечения информационной безопасности информационных систем, составлять аналитические обзоры по вопросам обеспечения информационной безопасности информационных систем
<b>Владеть:</b>	
Уровень 1	навыками анализа информационной инфраструктуры информационной системы и ее безопасности
Уровень 2	методами мониторинга и аудита, выявления угроз информационной безопасности информационных систем
Уровень 3	навыками участия в экспертизе состояния защищенности информации на объекте защиты

**ПК-10: способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности**

<b>Знать:</b>	
Уровень 1	основы методик анализа информационной безопасности объектов и систем
Уровень 2	-
Уровень 3	-
<b>Уметь:</b>	
Уровень 1	-
Уровень 2	-
Уровень 3	-
<b>Владеть:</b>	
Уровень 1	-
Уровень 2	-
Уровень 3	-

**ПК-15: способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю**

<b>Знать:</b>	
Уровень 1	основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации
Уровень 2	правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны и служб защиты информации на предприятиях
Уровень 3	организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации
<b>Уметь:</b>	
Уровень 1	применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности
Уровень 2	разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации
Уровень 3	определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите
<b>Владеть:</b>	
Уровень 1	навыками работы с нормативными правовыми актами
Уровень 2	навыками организации и обеспечения режима секретности
Уровень 3	методами формирования требований по защите информации

**ПСК-1: способностью формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности**

<b>Знать:</b>	
Уровень 1	цели, задачи, принципы и основные направления обеспечения информационной безопасности государства
Уровень 2	-
Уровень 3	-
<b>Уметь:</b>	
Уровень 1	пользоваться современной научно-технической информацией по исследуемым проблемам и задачам
Уровень 2	-
Уровень 3	-
<b>Владеть:</b>	
Уровень 1	навыками работы с нормативными правовыми актами
Уровень 2	-
Уровень 3	-

**В результате освоения дисциплины обучающийся должен**

<b>3.1</b>	<b>Знать:</b>
3.1.1	место и роль информационной безопасности в системе национальной безопасности Российской Федерации;
3.1.2	основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы по техническому и экспортному контролю в данной области; правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны;

3.1.3	систему сертификации средств защиты информации; принципы и методы организационной защиты информации.
<b>3.2</b>	<b>Уметь:</b>
3.2.1	пользоваться нормативными документами по защите информации; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем.
<b>3.3</b>	<b>Владеть:</b>
3.3.1	навыками организации и обеспечения режима секретности;
3.3.2	навыками работы с нормативными правовыми актами; методами организации и управления деятельностью служб защиты информации на предприятии;
3.3.3	профессиональной терминологией;
3.3.4	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
	<b>Раздел 1. Правовое обеспечение информационной безопасности</b>					
1.1	Информационные отношения как объект правового регулирования. Законодательство Российской Федерации в области информационной безопасности /Лек/	5	1	ОПК-5	Л1.1Л2.1 Л2.2 Л2.3 Э2 Э3	
1.2	Функции и полномочия ФСТЭК России, ФСБ России, Межведомственной комиссии по защите государственной тайны. /Пр/	5	2	ОПК-5 ПК-9	Л2.1 Л2.2 Л2.3Л3.3 Э1 Э3 Э4 Э5 Э6	Анализ практико-ориентированных задач. Групповая дискуссия
1.3	Законодательство РФ в области защиты ГТ /Пр/	5	2	ОПК-5 ПК-9	Л2.1 Л2.2 Л2.3Л3.3 Э1 Э2 Э3 Э5 Э6	Анализ практико-ориентированных задач. Групповая дискуссия
1.4	Подготовка к практическим занятиям /Ср/	5	8	ПК-15 ПСК-1	Л1.1Л2.1 Л2.2 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13 Л2.14 Л2.15 Л2.16 Л2.17 Л2.18 Л2.3Л3.1 Л3.3 Э1 Э2 Э3 Э4 Э5 Э6	
1.5	Правовой режим защиты государственной тайны /Лек/	5	1	ОПК-5	Л1.1Л2.1 Л2.2 Л2.3 Э1 Э5 Э6	
1.6	Подготовка к практическим занятиям /Ср/	5	8	ПК-15 ПСК-1	Л1.1Л2.1 Л2.2 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13 Л2.14 Л2.15 Л2.16 Л2.17 Л2.18 Л2.3Л3.1 Л3.3 Э1 Э2 Э3 Э4 Э5 Э6	
1.7	Правовые режимы защиты информации конфиденциального характера /Лек/	5	2	ОПК-5	Л1.1Л2.1 Л2.2 Л2.3 Э1 Э5 Э6 Э7	

1.8	Законодательство РФ в области защиты информации конфиденциального характера /Пр/	5	2	ОПК-5 ПК-9	Л2.1 Л2.2 Л2.3Л3.3 Э1 Э4 Э5	Анализ практико-ориентированных задач. Групповая дискуссия
1.9	Подготовка к практическим занятиям /Ср/	5	8	ПК-15 ПСК-1	Л1.1Л2.1 Л2.2 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13 Л2.14 Л2.15 Л2.16 Л2.17 Л2.18 Л2.3Л3.1 Л3.3 Э1 Э2 Э3 Э4 Э5 Э6	
1.10	Государственное регулирование деятельности в области защиты информации /Лек/	5	2	ОПК-5	Л1.1Л2.1 Л2.2 Л2.3 Э1 Э5 Э6	
1.11	Правовая защита служебной, профессиональной и коммерческой тайны /Пр/	5	2	ОПК-5 ПК-9 ПСК-1	Л2.1 Л2.2 Л2.3Л3.3 Э1 Э2 Э3 Э5	Анализ практико-ориентированных задач. Групповая дискуссия
1.12	Подготовка к практическим занятиям /Ср/	5	8	ПК-15 ПСК-1	Л1.1Л2.1 Л2.2 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13 Л2.14 Л2.15 Л2.16 Л2.17 Л2.18 Л2.3Л3.1 Л3.3 Э1 Э2 Э3 Э4 Э5 Э6	
1.13	Правовая охрана результатов интеллектуальной деятельности. /Лек/	5	2	ОПК-5	Л1.1Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3 Э5	
1.14	Подготовка к практическим занятиям /Ср/	5	8	ПК-15 ПСК-1	Л1.1Л2.1 Л2.2 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13 Л2.14 Л2.15 Л2.16 Л2.17 Л2.18 Л2.3Л3.1 Л3.3 Э1 Э2 Э3 Э4 Э5 Э6	
1.15	Преступления в сфере компьютерной информации /Лек/	5	1	ОПК-5	Л1.1Л2.1 Л2.2 Л2.3 Л2.5 Э1 Э2 Э3 Э4 Э5 Э6	
1.16	Правовая защита персональных данных /Пр/	5	2	ОПК-5 ПК-9 ПСК-1	Л2.1 Л2.2 Л2.3Л3.3 Э1 Э2 Э3 Э5 Э6	Анализ практико-ориентированных задач. Групповая дискуссия

1.17	Подготовка к практическим занятиям /Ср/	5	8	ПК-15 ПСК-1	Л1.1Л2.1 Л2.2 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13 Л2.14 Л2.15 Л2.16 Л2.17 Л2.18 Л2.3Л3.1 Л3.3 Э1 Э2 Э3 Э4 Э5 Э6	
	<b>Раздел 2. Организационное обеспечение информационной безопасности</b>					
2.1	Понятие организационной защиты информации /Лек/	5	2	ОПК-5	Л1.1Л2.1 Л2.2 Л2.3 Э1 Э2 Э3 Э4 Э5	
2.2	Лицензирование и сертификация в области ЗИ /Пр/	5	1	ОПК-5 ПК-9 ПСК-1	Л2.1 Л2.2 Л2.3Л3.3 Э1 Э2 Э3 Э4 Э5 Э6	Анализ практико-ориентиро ванных задач. Групповая дискуссия
2.3	Подготовка к практическим занятиям /Ср/	5	8	ПК-15 ПСК-1	Л1.1Л2.1 Л2.2 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13 Л2.14 Л2.15 Л2.16 Л2.17 Л2.18 Л2.3Л3.1 Л3.3 Э1 Э2 Э3 Э4 Э5 Э6	
2.4	Методы обеспечения физической безопасности. /Лек/	5	1	ОПК-5	Л1.1Л2.1 Л2.2 Л2.3 Э1 Э2 Э3 Э5 Э6 Э7	
2.5	Подготовка к практическим занятиям /Ср/	5	8	ПК-15 ПСК-1	Л1.1Л2.1 Л2.2 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13 Л2.14 Л2.15 Л2.16 Л2.17 Л2.18 Л2.3Л3.1 Л3.3 Э1 Э2 Э3 Э4 Э5 Э6	
2.6	Служба безопасности предприятия /Пр/	5	1	ОПК-5 ПК-9 ПСК-1	Л2.1 Л2.2 Л2.3Л3.3 Э1 Э2 Э3 Э5 Э6	Анализ практико-ориентиро ванных задач. Групповая дискуссия
2.7	Подготовка к практическим занятиям /Ср/	5	8	ПК-15 ПСК-1	Л1.1Л2.1 Л2.2 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13 Л2.14 Л2.15 Л2.16 Л2.17 Л2.18 Л2.3Л3.1 Л3.3 Э1 Э2 Э3 Э4 Э5 Э6	

2.8	Технологические меры поддержания безопасности /Лек/	5	2	ОПК-5	Л1.1Л2.1 Л2.2 Л2.3 Э1 Э2 Э3 Э5 Э6 Э7	
2.9	Резервирование оборудования и дублирование информации /Пр/	5	2	ОПК-5 ПК-9 ПСК-1	Л2.1 Л2.2 Л2.3Л3.3 Э1 Э2 Э3 Э5 Э6	Анализ практико-ориентирова нных задач. Групповая дискуссия
2.10	Организация режима секретности /Лек/	5	2	ОПК-5	Л1.1Л2.1 Л2.2 Л2.3 Э1 Э2 Э3 Э5 Э6	
2.11	Аттестация объектов информатизации /Пр/	5	2	ОПК-5 ПК-5 ПК-9 ПСК-1 ПК-10	Л2.1 Л2.2 Л2.3Л3.3 Э1 Э2 Э3 Э5 Э6	Анализ практико-ориентирова нных задач. Групповая дискуссия
2.12	Допуск к государственной тайне /Лек/	5	2	ОПК-5	Л1.1Л2.1 Л2.2 Л2.3 Э1 Э5 Э6	
2.13	Контроль доступа и средства поиска и досмотра. Системы контроля доступа. /Пр/	5	2	ОПК-5 ПК-9 ПСК-1	Л2.1 Л2.2 Л2.3Л3.3 Э1 Э2 Э3 Э5	Анализ практико-ориентирова нных задач. Групповая дискуссия
2.14	Выполнение и подготовка к защите курсовой работы /Ср/	5	36	ОПК-5 ПК-9 ПСК-1 ПК-10	Л1.1Л2.1 Л2.2 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13 Л2.14 Л2.15 Л2.16 Л2.17 Л2.18 Л2.3 Л2.4 Л2.5Л3.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7	
2.15	Промежуточная аттестация /Экзамен/	5	36	ОПК-5 ПК-5 ПК-9 ПК-15 ПСК-1 ПК-10	Л1.1Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2 Э3 Э4 Э5 Э6	

### 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
--	---------------------	----------	----------------------	------------



	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
Л1.1	Чукалова Л. Г., Ганженко Н.	Организационное и правовое обеспечение информационной безопасности: конспект лекций для студентов направления подготовки 10.03.01 «Информационная безопасность»	Екатеринбург: УрГУПС, 2016	<a href="http://biblioserver.usurt.ru/cgi-bin/irbis64r_13/cgiirbis_64.exe?C21COM=F&amp;I21DBN=KN&amp;P21DBN=KN">http://biblioserver.usurt.ru/cgi-bin/irbis64r_13/cgiirbis_64.exe?C21COM=F&amp;I21DBN=KN&amp;P21DBN=KN</a>
<b>6.1.2. Дополнительная учебная литература</b>				
	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	Стрельцов А. А.	Организационно-правовое обеспечение информационной безопасности: учебное пособие для студентов вузов, обучающихся по специальностям 090102 "Компьютерная безопасность", 090105 "Комплексное обеспечение информационной безопасности автоматизированных систем", 090106 "Информационная безопасность телекоммуникационных систем"	Москва: Академия, 2008	
Л2.4		Гражданский кодекс Российской Федерации: [официальный текст : текст Кодекса приводится по состоянию на 14 апреля 2011 г.]	Москва: ОМЕГА-Л, 2011	
Л2.5	Рос. Федерация	Уголовный кодекс Российской Федерации: [официальный текст : текст Кодекса приводится по состоянию на 20 сентября 2011 г.]	Москва: ОМЕГА-Л, 2011	
Л2.6		Положение о Федеральной службе по техническому и экспортному контролю	утв. Указом Президента РФ от 16 августа 2004 г. N 1085	<a href="http://ivo.garant.ru/#/document/12136635/paragraph/1950:35">http://ivo.garant.ru/#/document/12136635/paragraph/1950:35</a>
Л2.7		Положение о Федеральной службе безопасности и Российской Федерации	утв. Указом Президента РФ от 11 августа 2003 г. N 960	<a href="http://ivo.garant.ru/#/document/12132066/paragraph/27732:38">http://ivo.garant.ru/#/document/12132066/paragraph/27732:38</a>
Л2.8		Закон РФ от 21 июля 1993 г. N 5485-1 "О государственной тайне" (с изменениями и дополнениями)		<a href="http://ivo.garant.ru/#/document/10102673/paragraph/198:41">http://ivo.garant.ru/#/document/10102673/paragraph/198:41</a>
Л2.9		Указ Президента РФ от 6 марта 1997 г. N 188 "Об утверждении перечня сведений конфиденциального характера" (с изменениями и дополнениями)		<a href="http://ivo.garant.ru/#/document/10200083/paragraph/8885:43">http://ivo.garant.ru/#/document/10200083/paragraph/8885:43</a>
Л2.10		Федеральный закон от 27 июля 2006 г. N 152-ФЗ "О персональных данных" (с изменениями и дополнениями)		<a href="http://ivo.garant.ru/#/document/12148567/paragraph/24880:45">http://ivo.garant.ru/#/document/12148567/paragraph/24880:45</a>
Л2.11		Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных	утв. ФСТЭК России, 14.02.2008 г.	<a href="https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/380-metodika-opredeleniya-aktualnykh-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-fstek-rossii-2008-god">https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/380-metodika-opredeleniya-aktualnykh-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-fstek-rossii-2008-god</a>
Л2.12		Федеральный закон от 29 июля 2004 г. N 98-ФЗ "О коммерческой тайне" (с изменениями и дополнениями)		<a href="http://ivo.garant.ru/#/document/12136454/paragraph/12089:48">http://ivo.garant.ru/#/document/12136454/paragraph/12089:48</a>

Л2.13		Федеральный закон от 4 мая 2011 г. N 99-ФЗ "О лицензировании отдельных видов деятельности" (с изменениями и дополнениями)		<a href="http://ivo.garant.ru/#/document/12185475/paragraph/5637:50">http://ivo.garant.ru/#/document/12185475/paragraph/5637:50</a>
Л2.14		Федеральный закон от 27 декабря 2002 г. N 184-ФЗ "О техническом регулировании" (с изменениями и дополнениями)		<a href="http://ivo.garant.ru/#/document/12129354/paragraph/157574:53">http://ivo.garant.ru/#/document/12129354/paragraph/157574:53</a>
Л2.15		Защита информации. Инсайд: специализированное отечественное периодическое издание	Издательский Дом «Афина»	<a href="https://elibrary.ru/title_about.asp?id=25917">https://elibrary.ru/title_about.asp?id=25917</a>
Л2.16		Вестник УрФО. Безопасность в информационной сфере: специализированное отечественное периодическое издание	Изд-во ЮУрГУ	<a href="https://elibrary.ru/title_about.asp?id=32751">https://elibrary.ru/title_about.asp?id=32751</a>
Л2.17		Безопасность информационных технологий: специализированное отечественное периодическое издание	Изд-во Национального исследовательского ядерного университета «МИФИ»	<a href="https://elibrary.ru/title_about.asp?id=8429">https://elibrary.ru/title_about.asp?id=8429</a>
Л2.18		Каталог учебных, учебно-методических пособий, научных и других изданий вузов железнодорожного транспорта: справочно-библиографическое издание	Москва, ФГБУ ДПО «УМЦ ЖДТ» 2018	<a href="http://www.usurt.ru/izdatelsko-bibliotchnyy-kompleks/bibliotchno-informacionnuy-center/katalog-fgbou-umts-zhdt">http://www.usurt.ru/izdatelsko-bibliotchnyy-kompleks/bibliotchno-informacionnuy-center/katalog-fgbou-umts-zhdt</a>

Специализированные зарубежные периодические издания в области информационной безопасности при изучении данной дисциплины не используются

### 6.1.3. Методические разработки

	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
Л3.1	Чукалова Л. Г., Ганженко Н.	Организационное и правовое обеспечение информационной безопасности: методические рекомендации по организации самостоятельной работы студентов направления подготовки 10.03.01 «Информационная безопасность»	Екатеринбург: УрГУПС, 2016	<a href="http://biblioserver.usurt.ru/cgi-bin/irbis64r_13/cgiirbis_64.exe?C21COM=F&amp;I21DBN=KN&amp;P21DBN=KN">http://biblioserver.usurt.ru/cgi-bin/irbis64r_13/cgiirbis_64.exe?C21COM=F&amp;I21DBN=KN&amp;P21DBN=KN</a>
Л3.2	Чукалова Л. Г.	Организационное и правовое обеспечение информационной безопасности: методические рекомендации к выполнению курсовой работы для студентов направления подготовки 10.03.01 «Информационная безопасность»	Екатеринбург: УрГУПС, 2016	<a href="http://biblioserver.usurt.ru/cgi-bin/irbis64r_13/cgiirbis_64.exe?C21COM=F&amp;I21DBN=KN&amp;P21DBN=KN">http://biblioserver.usurt.ru/cgi-bin/irbis64r_13/cgiirbis_64.exe?C21COM=F&amp;I21DBN=KN&amp;P21DBN=KN</a>
Л3.3	Чукалова Л. Г., Ганженко Н.	Организационное и правовое обеспечение информационной безопасности: методические рекомендации к практическим занятиям для студентов направления подготовки 10.03.01 «Информационная безопасность»	Екатеринбург: УрГУПС, 2016	<a href="http://biblioserver.usurt.ru/cgi-bin/irbis64r_13/cgiirbis_64.exe?C21COM=F&amp;I21DBN=KN&amp;P21DBN=KN">http://biblioserver.usurt.ru/cgi-bin/irbis64r_13/cgiirbis_64.exe?C21COM=F&amp;I21DBN=KN&amp;P21DBN=KN</a>

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

Э1	Официальный сайт ФСТЭК России ( <a href="http://www.fstec.ru">http://www.fstec.ru</a> )
Э2	Информационный бюллетень компании "Инфосистемы Джет" ( <a href="http://www.jetinfo.ru">http://www.jetinfo.ru</a> )
Э3	SecurityLab.ru - информационный портал, оперативно и ежедневно рассказывающий о событиях в области защиты информации, интернет права и новых технологиях ( <a href="http://www.securitylab.ru">http://www.securitylab.ru</a> )
Э4	Интернет портал ISO27000.RU (ЗАЩИТА-ИНФОРМАЦИИ.SU) ( <a href="http://iso27000.ru">http://iso27000.ru</a> )
Э5	Система электронной поддержки обучения Blackboard Learn ( <a href="http://bb.usurt.ru">http://bb.usurt.ru</a> )
Э6	Официальный сайт ФСБ России ( <a href="http://www.fsb.ru">http://www.fsb.ru</a> )
Э7	Официальный сайт ОАО "Российские железные дороги" ( <a href="http://www.rzd.ru">http://www.rzd.ru</a> )

<b>6.3 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем</b>	
<b>6.3.1 Перечень программного обеспечения</b>	
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
<b>6.3.2 Перечень информационных справочных систем и профессиональных баз данных</b>	
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: <a href="https://bdu.fstec.ru/">https://bdu.fstec.ru/</a>
6.3.2.5	Государственный реестр сертифицированных средств защиты информации N РОСС RU.0001.01БИ00
6.3.2.6	Международная реферативная база данных научных изданий eLIBRARY.RU

**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
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
Учебная аудитория для проведения групповых и индивидуальных консультаций	Специализированная мебель
Компьютерный класс - Учебная аудитория для курсового проектирования (выполнения курсовых работ), самостоятельной работы студентов, для проведения групповых и индивидуальных консультаций	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

**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](http://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](http://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](http://bb.usurt.ru)).