Модуль 1

Нормативно-правовая база обеспечения безопасности информационных технологий

1. Цели освоения дисциплины

Целью освоения дисциплины «Нормативно-правовая база обеспечения безопасности информационных технологий» является: формирование знаний в законодательства в информационной сфере и применения современных подходов к регламентации деятельности в области информационной безопасности..

2.Место дисциплины в структуре ДПП

Дисциплина «Нормативно-правовая база обеспечения безопасности информационных технологий» относится к первому разделу (модуль 1) ДПП.

Знания, умения и навыки, полученные в процессе изучения дисциплины «Нормативно-правовая база обеспечения безопасности информационных технологий», в дальнейшем используются в процессе самостоятельной исследовательской и практической работе слушателей, а также при изучении остальных дисциплин курса.

3. Перечень планируемых результатов обучения по дисциплине (модулю) соотнесенных с планируемыми результатами освоения программы

Имеющаяся квалификация и (или) уровень образования (при наличии) соответствующего требования к слушателям:

Виды деятельности	Профессиональные компетенции или трудовые функции	Практический опыт	Умения	Знания
Организационно-управленческая	ПК-4 способностью использовать основы правовых знаний в различных сферах деятельности	**1.** методикой правового анализа норм, составляющих систему информационного права	2. применять методы и средства познания для интеллектуального развития, повышения культурного уровня, 3. профессиональной компетентности; использовать правовые нормы в профессиональной деятельности; 4. ориентироваться в системе законодательства и нормативно-правовых актов, регулирующих сферу профессиональной деятельности; **5.** защищать	1. понятие, предмет и метод информационного права, 2. информационно-правовые нормы и отношения, источники информационного права, **3.** государственную политику информатизации

			права на интеллектуальную собственность	

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 60 часов.

4.1. Содержание разделов дисциплины

Форма обучения заочная (очно-заочная)

№ п/п	Раздел и тема дисциплины	Семестр	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)			Формы текущего контроля успеваемости
			Лекции	Семинар Лаборат. Практич.	Самост. раб.	
1	Законодательство в области информационной безопасности и его система.	1	2	-	18	Выполнение тестовых заданий
2	Правовое обеспечение информационной безопасности.	1	2	-	18	Выполнение тестовых заданий
3	Юридическая ответственность за нарушения законодательства в области информационной безопасности	1	2	-	18	Выполнение тестовых заданий
	ИТОГО		**6**	**-**	**54**	

4.2. Лекционные занятия, их содержание

№ п/п	Наименование разделов и тем	Содержание
1	1. Законодательство в области информационной безопасности и его система.	Понятие информационного законодательства. Понятие системы информационного законодательства. Структура информационного законодательства. Общая характеристика информационного законодательства. Действие нормативных правовых актов в информационной сфере во времени, в пространстве и по кругу лиц.
2	2. Правовое обеспечение информационной безопасности.	Понятие и общая характеристика информационной безопасности. Основные задачи по обеспечению информационной безопасности. Методы обеспечения информационной безопасности. Особенности обеспечения информационной безопасности

		Российской Фе-дерации в экономической сфере. Особенности обеспечения информационной безопасности в сфере внутренней политики. Особенности обеспечения информационной безопасно-сти в сфере внешней политики. Особенности обеспечения информационной безопасности в сфере науки и техники. Особенности обеспечения информационной безопасности в сфе-ре общегосударственных информационных и телекоммуникационных систем. Основные положения государственной политики обеспечения информационной безопасности Рос-сии. Организационная основа системы обеспечения информационной безопасности РФ
3	3. Юридическая ответственность за нарушения законодательства в области информационной безопасности	Понятие и общая характеристика юридической ответственности за нарушение зако-нодательства в информационной сфере. Дисциплинарная ответственность за правонару-шения в информационной сфере, понятие и общая характеристика. Гражданско-правовая ответственность за правонарушения в информационной сфере, понятие и общая характе-ристика. Административная ответственность за нарушение законодательства в информа-ционной сфере. Уголовная ответственность за совершение преступлений в информацион-ной сфере, понятие и общая характеристика.

4.3. Семинарские, практические, лабораторные занятия, их содержание

Не предусмотрены

4.4 Вид и форма промежуточной аттестации

Промежуточный контроль проводится в форме зачета.

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

В процессе самостоятельной работы обучающиеся, помимо основной и дополнительной литературы, рекомендованной в п.7, могут пользоваться следующими методическими материалами:

- Практикумы, сборники задач;
- Прочее

6. Оценочные средства для проведения промежуточной аттестации по дисциплине

6.1. Текущий контроль

6.1.1. Образцы тестовых и контрольных заданий текущего контроля

Комплект тестовых заданий

1. Обработка специальных категорий персональных данных в отношении религиозных или философских убеждений допускается в случае, когда обработка персональных данных

– осуществляется в медицинских целях для установления диагноза при условии, что ее осуществляет профессиональный медицинский работник
– необходима в связи с осуществлением правосудия
– необходима в связи с выездом за пределы Российской Федерации

– необходима в соответствии с оперативно-розыскной деятельностью

2. Учредителями средства массовой информации могут выступать

– только юридические лица
– граждане другого государства, постоянно не проживающие в Российской Федерации, юридические лица и органы государственной власти
– граждане, достигшие 18 лет и лица без гражданства, постоянно проживающие на территории Российской Федерации
– граждане, достигшие 18 лет, объединения граждан, организаций, органы государственной власти
– граждане, достигшие 16 лет и юридические лица

3. С точки зрения информационного права информация – это

– сведения независимо от формы их представления
– сведения о законодательстве, правовых явлениях, правоприменительной деятельности
– форма выражения объективных знаний
– данные о развитии конкретной правовой науки и ее практическом применении

4. Режим общественного достояния устанавливается для

– любой общественной организации
– для государственных органов и муниципальных образований
– любой общедоступной информации
– сведений, которые являются уникальными, незаменимыми по своей природе

5. Исключите неправильный постулат

– информация не связана с определенным конкретным носителем
– информация не существует без материального носителя
– содержание информации меняется одновременно со сменой материального носителя

6. Предмет информационного права на современном этапе развития законодательства – это

– общественные отношения в информационной сфере
– продукты, производные от информации и деятельность, связанная с ними
– совокупность результатов труда, воплощенных в информации, информационных ресурсов, информационных технологий, средств и технологий коммуникации информации по сетям связи
– информационные отношения, возникающие в процессе производства, сбора, обработки, накопления, хранения, поиска, передачи, распространения и потребления информации

7. Режим документированной информации – это

– выделенная информация по определенной цели
– выделенная информация в любой знаковой форме
– электронная информация, позволяющая ее идентифицировать
– электронный документ с электронной подписью

8. Под периодическим печатным изданием понимается альманах, бюллетень, имеющие

– постоянное название, текущий номер и выходящие в свет не реже одного раза в год
– постоянное название и выходящие в свет не реже одного раза в месяц
– постоянное название и текущий номер
– постоянное название, текущий номер и выходящие в свет не реже одного раза в месяц

9. В регистрации средства массовой информации не может быть отказано

– по мотивам нецелесообразности
– даже если сведения в заявлении не соответствуют действительности
– когда заявление подано не соответствующим лицом
– если регистрирующий орган уже зарегистрировал другое средство массовой информации с тем же названием и формой распространения

10. Основное средство антивирусной защиты

- резервное копирование ценных данных
- подготовка квалифицированных кадров в сфере информационной безопасности
- регулярное сканирование жестких дисков

6.2. Промежуточный контроль *(зачет)*

6.2.1. Перечень вопросов к зачету

1.Информационное общество. Предмет ИП.
2.Объект правового регулирования и сфера действия ИП.
3.Формирование правосознания в информационной сфере.
4.Виды субъектов информационного права.
5.Информационная деятельность как основа правоотношений.
6.Состояние разработки проблемы о праве на информацию.
7.Какая информация может быть использована для коммерческого распространения и что является источником получения прибыли при продаже информации?
8.Правовое обеспечение деятельности операторов в процессе трансграничного обмена электронными документами.
9.Правовой режим информационных ресурсов.
10.Международный обмен информацией.
11.Электронное правительство как развитие идей электронной демократии.
12.Правовое обеспечение Интернет.
13.Проблемы Интернета в России и за рубежом.
14.Проблемы, оставшиеся после принятия части четвертой ГК РФ.
15.Системы правовой информации.
16.Психические вирусы.
17.Информационные права человека.
18.Федеральный закон от 27 июля 2006 года No 149-ФЗ "Об информации, информационных технологиях и о защите информации".
19.Федеральный закон от 10 января 2002 г. No 1-ФЗ "Об электронной цифровой подписи".
20.Персональные базы данных, проблема «расколотых» баз.
21.Журналист как субъект информационного права.
22.Информационные экологические права человека.
23.Консциентальные войны.
24.Правовое обеспечение электронной коммерции.
25.Современное понимание электронной торговли, факторы рационального потребления в информационном обществе.
26.Правовое регулирование договорных отношений в сфере электронной торговли.
27.Концепция сетевого договора.
28.Интернет-торговля.
29.Обзор систем электронного голосования в различных странах.
30.Информационно-правовое обеспечение институтов международных наблюдателей.
31.Виды интернет голосования.
32.Государственная автоматизированная система «Выборы».
33.Информационные войны.
34.Государственная политика в области доступа к правовым базам данных.
35.Перспективы развития правовых баз данных.
36.Электронный нотариат.
37.Внедрение электронного здравоохранения.
38.Кодекс этики телемедицины.
39.Федеральный закон от 27 июля 2006 года No 152-ФЗ "О персональных данных".
40.Проблемы Интернета в России и за рубежом.
41.Механизм защиты частной жизни потребителя.
42.Орган, гарантирующий международную защиту свободы выражения мнений, -Европейский суд по правам человека в Страсбурге. Применение Европейским судом статьи 10 Европейской конвенции по правам человека.
43.Международно-правовая практика обеспечения свободы информации. Правовое оформление понятия свободы самовыражения в международных актах.
44.Правовое регулирование Интернет в странах Европы, США, России. Диффамация, принцип Салливана.
45.Доступ к судебным слушаниям. Информационное законодательство в Великобритании. Место международных соглашений о правах человека в национальном праве в Великобритании.
46.Информационное законодательство в Федеративной Республике Германии.
47.Французское законодательство о средствах массовой информации. Конституция Франции и другие источники права СМИ.

48.Законодательство о средствах массовой информации в Австрии. Место международных соглашений о правах человека в национальном праве в Австрии.

49.Сравнительная характеристика законодательства СМИ за рубежом и в России. Информационная безопасность и дипломатическая служба России.

50.Интернет как механизм общественного контроля

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

а) основная литература:

	Год издания	Вид (бум., электр.)	Количество экз. (для электронных изданий – эл. адрес)
Общество с ограниченной ответственностью "СТАТУТ"	2019	электр.	https://e.lanbook.com/book/130674
Ставропольский государственный аграрный университет	2015	электр.	https://e.lanbook.com/book/82215
Ставропольский государственный аграрный университет	2015	электр.	https://e.lanbook.com/book/82216

б) дополнительная литература:

Наименование, издательство	Год издания	Вид (бум., электр.)	Количество экз. (для электронных изданий – эл. адрес)
Санкт-Петербург, Лань	2020	электр.	https://e.lanbook.com/reader/book/130184
Дашков и К, Ай Пи Эр Медиа	2016	электр.	http://www.iprbookshop.ru/57155.html
Ай Пи Эр Медиа	2016	электр.	http://www.iprbookshop.ru/59275.html
Феникс	2015	электр.	http://www.iprbookshop.ru/59353.html

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к нескольким электронно-библиотечным системам (электронным библиотекам)*:*

– «Университетская библиотека онлайн» ООО «Директ-Медиа», адрес доступа: www.biblioclub.ru, доступ круглосуточный неограниченный из любой точки Интернет при условии регистрации в БГУ;

– Универсальная справочно-информационная полнотекстовая база данных ООО «ИВИС», адрес доступа: www.ebiblioteka.ru, доступ круглосуточный неограниченный из любой точки Интернет при условии регистрации в БГУ;

– Электронная библиотека Издательского дома «Гребенников», адрес доступа: www.grebennikon.ru; доступ с компьютеров сети БГУ (по IP-адресам)

– Научная электронная библиотека «Киберленинка», адрес доступа: http://cyberleninka.ru, доступ круглосуточный, неограниченный для всех пользователей, бесплатное чтение и скачивание всех научных публикаций, в том числе пакет «Юридические науки», коллекция из 7 журналов по правоведению;

– НЭБ «eLibrary», адрес доступа: www.elibrary.ru, доступ к российским журналам, находящимся полностью или частично в открытом доступе при условии регистрации;

– Информационная система «Единое окно доступа к образовательным ресурсам», поставщик – Федеральное государственное автономное учреждение «Государственный научно-исследовательский институт информационных технологий и телекоммуникаций», адрес доступа: http://window.edu.ru, доступ свободный к интегральному каталогу образовательных Интернет-ресурсов и к электронной библиотеке учебно-методических материалов для общего и профессионального образования, доступ круглосуточный неограниченный для всех пользователей;

– Изд-во «Лань», адрес доступа: http://e.lanbook.com, бесплатный полнотекстовый доступ к 7 коллекциям издательства;

9. Методические указания для обучающихся по освоению дисциплины (модуля)

Изучать дисциплину рекомендуется в соответствии с той последовательностью, которая обозначена в ее содержании.

На лекциях преподаватель озвучивает тему, знакомит с перечнем литературы по теме, обосновывает место и роль этой темы в данной дисциплине, раскрывает ее практическое значение. В ходе лекций обучающемуся необходимо вести конспект, фиксируя основные понятия и проблемные вопросы.

Практические занятия по своему содержанию связаны с тематикой лекционных занятий. Начинать подготовку к занятию целесообразно с конспекта лекций. Задание на практическое занятие сообщается обучающимся до его проведения.

Изучение дисциплины (модуля) включает самостоятельную работу обучающегося.

Основными видами самостоятельной работы обучающихся с участием преподавателей являются:

- текущие консультации;

Основными видами самостоятельной работы обучающихся без участия преподавателей являются:

- формирование и усвоение содержания конспекта лекций на базе рекомендованной лектором учебной литературы, включая информационные образовательные ресурсы (электронные учебники, электронные библиотеки и др.);
- самостоятельное изучение отдельных тем или вопросов по учебникам или учебным пособиям;
- выполнение домашних заданий в виде решения отдельных задач, проведения типовых расчетов, расчетно-компьютерных и индивидуальных работ по отдельным разделам содержания дисциплин и др.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационно-справочных систем (при *необходимости)*:

В учебном процессе, помимо полного пакета Microsoft Office 2016, используется специализированное программное обеспечение:

7-Zip

Пакет OpenOffice

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю):

- лекционные аудитории;
- аудитории для проведения семинарских и практических занятий;
- мультимедийные аудитории, оборудованные интерактивными досками;

Модуль 2

Методология обеспечения информационной безопасности

1. Цели освоения дисциплины

Целью освоения дисциплины «Методология обеспечения информационной безопасности» является: формирование знаний в области средств и методик обеспечения информационной безопасности.

2.Место дисциплины в структуре ДПП

Дисциплина «Методология обеспечения информационной безопасности» относится ко второму разделу (модуль 2) ДПП.

Знания, умения и навыки, полученные в процессе изучения дисциплины «Методология обеспечения информационной безопасности», в дальнейшем используются в процессе самостоятельной исследовательской и практической работе слушателей, а также при изучении остальных дисциплин курса.

3. Перечень планируемых результатов обучения по дисциплине (модулю) соотнесенных с планируемыми результатами освоения программы

Имеющаяся квалификация и (или) уровень образования (при наличии) соответствующего требования к слушателям:

Виды деятельности	Профессиональные компетенции или трудовые функции	Практический опыт	Умения	Знания
Научно-исследовательская	ПК-26 - понимание теоретических основ и общих принципов использования управления безопасностью ИТ	выполнять полный объем работ, связанных с комплексным обеспечением информационной безопасности конкретных автоматизированных систем на основе разработанных программ и методик	Правильно проводить анализ угроз информационной безопасности, выполнять основные этапы решения задач информационной на практике основные общеметодологические принципы теории информационной безопасности.	Терминологию в области информационной безопасности, методы и средства обеспечения информационной безопасности, методы нарушения конфиденциальности, целостности и доступности информации.

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 60 часов.

4.1. Содержание разделов дисциплины

Форма обучения заочная (очно-заочная)

№ п/п	Раздел и тема дисциплины	Семестр	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)			Формы текущего контроля успеваемости
			Лекции	Семинар Лаборат. Практич.	Самост. раб.	
1	Методы нарушения конфиденциальности, целостности и доступности информации	1	4	-	24	Выполнение тестовых заданий
2	Причины, виды, каналы утечки и искажения информации.	1	2	-	30	Выполнение тестовых заданий
	ИТОГО		**6**	**-**	**54**	

4.2. Лекционные занятия, их содержание

№ п/п	Наименование разделов и тем	Содержание
1	1. Методы нарушения конфиденциальности, целостности и доступности информации	Понятие конфиденциальности, целостности и доступности информации. Причины нарушения конфиденциальности, целостности и доступности информации. Аппаратные и программные методы борьбы с нарушениями конфиденциальности, целостности и доступности информации.
2	2. Причины, виды, каналы утечки и искажения информации	Причины искажения информации, их классификация, историческая ретроспектива, современное состояние. Виды искажения информации, классификация по целям и по методам. Понятие канала утечки и способы их идентификации, методы блокировки каналов утечки информации

4.3. Семинарские, практические, лабораторные занятия, их содержание

Не предусмотрены

4.4 Вид и форма промежуточной аттестации

Промежуточный контроль проводится в форме зачета.

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

В процессе самостоятельной работы обучающиеся, помимо основной и дополнительной литературы, рекомендованной в п.7, могут пользоваться следующими методическими материалами:

- Практикумы, сборники задач;
- Прочее

6. Оценочные средства для проведения промежуточной аттестации по дисциплине

6.1. Текущий контроль

6.1.1. Образцы тестовых и контрольных заданий текущего контроля

Комплект тестовых заданий

1. Основная масса угроз информационной безопасности приходится на
– Троянские программы
– Черви
– Шпионские программы
2. Какой вид идентификации и аутентификации получил наибольшее распространение?
– одноразовые пароли
– постоянные пароли
– системы PKI
3. Под какие системы распространение вирусов происходит наиболее динамично ?
– Windows
– Android
– Mac OS
4. Заключительным этапом построения системы защиты является
– анализ уязвимых мест
– планирование
– сопровождение
5. Какие угрозы безопасности информации являются преднамеренными ?
– Ошибки персонала
– Не авторизованный доступ
– Открытие электронного письма, содержащего вирус
6. Какого подход к обеспечению безопасности имеет место ?
– комплексный
– теоретический
– логический
7. Системой криптографической защиты информации является:
– Крипто Про
– BFox Pro
– CAudit Pro
8. Какие вирусы активизируются в самом начале работы с операционной системой ?
– троянцы
– загрузочные вирусы
– черви
9. Stuxnet это ...
– Промышленный вирус
– Троянская программа
– Макровирус
10. Таргетированная атака - ...
– Атака на конкретный компьютер пользователя
– Атака на компьютерную систему крупного предприятия
– Атака на сетевое оборудование

6.2. Промежуточный контроль *(зачет)*

6.2.1. Перечень вопросов к зачету

1. Основная идея теория информации по К. Шеннону, её отличие от семантической теории информации по Ю.А. Шрейдеру.
2. Виды информации, её свойства и особенности их взаимодействия.
3. Соотношение между материей и информацией.
4. Понятие информации по К. Шеннону и Н. Винеру.
5. Семантический, лингвистический, прагматический и технический аспекты информации.

6. Основные признаки информации.
7. Информация, данные и знание, их взаимосвязь и различие.
8. Основные документы, определяющие концептуальные основы информационнойбезопасности РФ.
9. Концепция национальной безопасности РФ. Важнейшие задачи обеспечения национальнойбезопасности в информационной сфере.
10. Доктрина информационной безопасности.
11. Понятие национальных интересов.
12. Национальные интересы страны в информационной сфере, угрозы национальныминтересам.
13. Причины и источники угроз национальным интересам страны.
14. Виды безопасности.
15. Национальная безопасность и её составляющие.
16. Субъекты системы и уровни обеспечения национальной безопасности РФ.
17. Основные задачи по обеспечению национальной безопасности.
18. Возможные сценарии подрыва безопасности России без применения военных средств.
19. Понятие "Информационной безопасности".
20. Место информационной безопасности в системе национальной безопасности России.
21. Важнейшие федеральные нормативные правовые акты, касающиеся информационнойбезопасности.
22. Законы, непосредственно касающиеся защиты компьютерной информации.
23. Информация и право. Информация как объект правового регулирования.
24. Информационные отношения.
25. Законы, действующие в области производства, распространения и потребленияинформации.
26. Информационная война, методы и средства её ведения.
27. Информационное оружие, его классификация и возможности.
28. Методы нарушения конфиденциальности, целостности и доступности информации.
29. Причины, виды, каналы утечки и искажения информации.
30. Основные направления обеспечения информационной безопасности объектовинформационной сферы.
31. Методы и средства обеспечения ИБ объектов информационной сферы.
32. Стандарты и нормативы в сфере обеспечения информационной безопасности.
33. Определение безопасности компьютерной системы и категории требований безопасности.
34. Базовые требования безопасности компьютерной системы.
35. Классы безопасности компьютерных систем, понятие риска.
36. Сущность понятий: "Вычислительная база защиты", "Монитор обращений", "Ядробезопасности".
37. Режимы функционирования компьютерной системы.
38. Сущность понятий: идентификация, аутентификация; авторизация.
39. Адекватность средств защиты.
40. Понятие продукта ИТ и системы обработки информации.

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

а) основная литература:

	Год издания	Вид (бум., электр.)	Количество экз. (для электронных изданий – эл. адрес)
Издательство "Лань"	2019	электр.	https://e.lanbook.com/book/114688
Издательство "Горячая линия-Телеком"	2018	электр.	https://e.lanbook.com/book/111075
Издательство "Лань"	2020	электр.	https://e.lanbook.com/book/133924

б) дополнительная литература:

Наименование, издательство	Год издания	Вид (бум., электр.)	Количество экз. (для электронных изданий – эл. адрес)
Издательство "ФЛИНТА"	2015	электр.	https://e.lanbook.com/book/62972
Вузовское образование	2018	электр.	http://www.iprbookshop.ru/77320.html
Интернет-Университет Информационных Технологий (ИНТУИТ)	2016	электр.	http://www.iprbookshop.ru/52209.html
Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа	2020	электр.	http://www.iprbookshop.ru/89443.html
Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование	2017	электр.	http://www.iprbookshop.ru/72341.html
Ай Пи Ар Букс	2015	электр.	http://www.iprbookshop.ru/33857.html

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к нескольким электронно-библиотечным системам (электронным библиотекам):

– «Университетская библиотека онлайн» ООО «Директ-Медиа», адрес доступа: www.biblioclub.ru, доступ круглосуточный неограниченный из любой точки Интернет при условии регистрации в БГУ;

– Универсальная справочно-информационная полнотекстовая база данных ООО «ИВИС», адрес доступа: www.ebiblioteka.ru, доступ круглосуточный неограниченный из любой точки Интернет при условии регистрации в БГУ;

– Электронная библиотека Издательского дома «Гребенников», адрес доступа: www.grebennikon.ru; доступ с компьютеров сети БГУ (по IP-адресам)

– Научная электронная библиотека «Киберленинка», адрес доступа: http://cyberleninka.ru, доступ круглосуточный, неограниченный для всех пользователей, бесплатное чтение и скачивание всех научных публикаций, в том числе пакет «Юридические науки», коллекция из 7 журналов по правоведению;

– НЭБ «eLibrary», адрес доступа: www.elibrary.ru, доступ к российским журналам, находящимся полностью или частично в открытом доступе при условии регистрации;

– Информационная система «Единое окно доступа к образовательным ресурсам», поставщик – Федеральное государственное автономное учреждение «Государственный научно-исследовательский институт информационных технологий и телекоммуникаций», адрес доступа: http://window.edu.ru, доступ свободный к интегральному каталогу образовательных Интернет-ресурсов и к электронной библиотеке учебно-методических материалов для общего и профессионального образования, доступ круглосуточный неограниченный для всех пользователей;

– Изд-во «Лань», адрес доступа: http://e.lanbook.com, бесплатный полнотекстовый доступ к 7 коллекциям издательства;

9. Методические указания для обучающихся по освоению дисциплины (модуля)

Изучать дисциплину рекомендуется в соответствии с той последовательностью, которая обозначена в ее содержании.

На лекциях преподаватель озвучивает тему, знакомит с перечнем литературы по теме, обосновывает место и роль этой темы в данной дисциплине, раскрывает ее практическое значение. В ходе лекций обучающемуся необходимо вести конспект, фиксируя основные понятия и проблемные вопросы.

Практические занятия по своему содержанию связаны с тематикой лекционных занятий. Начинать подготовку к занятию целесообразно с конспекта лекций. Задание на практическое занятие сообщается обучающимся до его проведения.

Изучение дисциплины (модуля) включает самостоятельную работу обучающегося.

Основными видами самостоятельной работы обучающихся с участием преподавателей являются:

- текущие консультации;

Основными видами самостоятельной работы обучающихся без участия преподавателей являются:

- формирование и усвоение содержания конспекта лекций на базе рекомендованной лектором учебной литературы, включая информационные образовательные ресурсы (электронные учебники, электронные библиотеки и др.);
- самостоятельное изучение отдельных тем или вопросов по учебникам или учебным пособиям;

- выполнение домашних заданий в виде решения отдельных задач, проведения типовых расчетов, расчетно-компьютерных и индивидуальных работ по отдельным разделам содержания дисциплин и др.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационно-справочных систем (при *необходимости)*:

В учебном процессе, помимо полного пакета Microsoft Office 2016, используется специализированное программное обеспечение:

7-Zip

Пакет OpenOffice

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю):

- лекционные аудитории;
- аудитории для проведения семинарских и практических занятий;
- мультимедийные аудитории, оборудованные интерактивными досками;

Модуль 3

Управление обеспечением безопасности информационных технологий

1. Цели освоения дисциплины

Целью освоения дисциплины «Управление обеспечением безопасности информационных технологий» является формирование теоретических навыков, умений И принципов осуществления деятельности по обеспечению безопасности информационных технологий.

2.Место дисциплины в структуре ДПП

Дисциплина «Методология обеспечения информационной безопасности» относится к третьему разделу (модуль 3) ДПП.

Знания, умения и навыки, полученные в процессе изучения дисциплины «Методология обеспечения информационной безопасности», в дальнейшем используются в процессе самостоятельной исследовательской и практической работе слушателей, а также при изучении остальных дисциплин курса.

3. Перечень планируемых результатов обучения по дисциплине (модулю) соотнесенных с планируемыми результатами освоения программы

Имеющаяся квалификация и (или) уровень образования (при наличии) соответствующего требования к слушателям:

Виды деятельности	Общепрофессиональные компетенции	Практический опыт	Умения	Знания
Научно-исследовательская	ОПК-1 способностью самостоятельно осуществлять научно-исследовательскую деятельность в соответствующей профессиональной области с использованием современных методов исследования и информационно-коммуникационных технологий	навыками оценки эффективности использования информационно-коммуникационных технологий в области организации информационной безопасности	проводить сравнительную оценку эффективности различных методов научных исследований и информационно-коммуникационных технологий в области организации информационной безопасности СЭИС	современные методы научных исследований и информационно-коммуникационных технологий в области организации информационной безопасности социально-экономических информационных систем (СЭИС).

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 60 часов.

4.1. Содержание разделов дисциплины

Форма обучения заочная (очно-заочная)

№ п/п	Раздел и тема дисциплины	Семестр	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)			Формы текущего контроля успеваемости
			Лекции	Семинар Лаборат. Практич.	Самост. раб.	
1	Современная нормативно-законодательная база обеспечения информационной безопасности.	1	2	-	18	Выполнение тестовых заданий
2	Анализ возможных нарушений и атак в социально-экономических информационных системах (СЭИС).	1	2	-	18	Выполнение тестовых заданий
3	Исследование влияния и противодействие вредоносным программам в СЭИС.	1	2	-	18	Выполнение тестовых заданий
	ИТОГО		**6**	**-**	**54**	

4.2. Лекционные занятия, их содержание

№ п/п	Наименование разделов и тем	Содержание
1	1. Современная нормативно-законодательная база обеспечения информационной безопасности.	Международная законодательная база обеспечения информационной безопасности, нормативные документы, стандарты и рекомендации, особенности их применения в российском правовом и информационном пространстве
2	2. Анализ возможных нарушений и атак в социально-экономических информационных системах (СЭИС).	Классификация нарушений и атак в социально-экономических системах. Методы анализа и обнаружения атак в социально-экономических системах
3	3. Исследование влияния и противодействие вредоносным программам в СЭИС.	Параметры влияния вредоносных программ, математическая оценка вероятности нарушений в социально-экономических информационных системах

4.3. Семинарские, практические, лабораторные занятия, их содержание

Не предусмотрены

4.4 Вид и форма промежуточной аттестации

Промежуточный контроль проводится в форме зачета.

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

В процессе самостоятельной работы обучающиеся, помимо основной и дополнительной литературы, рекомендованной в п.7, могут пользоваться следующими методическими материалами:

- Практикумы, сборники задач;
- Прочее

6. Оценочные средства для проведения промежуточной аттестации по дисциплине

6.1. Текущий контроль

6.1.1. Образцы тестовых и контрольных заданий текущего контроля

Комплект тестовых заданий

1. Кто является основным ответственным за определение уровня классификации информации?
– Руководитель среднего звена
– Высшее руководство
– Владелец
– Пользователь

2. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?
– Сотрудники
– Хакеры
– Атакующие
– Контрагенты (лица, работающие по договору)

3. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?
– Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования
– Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации
– Улучшить контроль за безопасностью этой информации
– Снизить уровень классификации этой информации

4. Что самое главное должно продумать руководство при классификации данных?
– Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным
– Необходимый уровень доступности, целостности и конфиденциальности
– Оценить уровень риска и отменить контрмеры
– Управление доступом, которое должно защищать данные

5. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?
– Владельцы данных
– Пользователи
– Администраторы
– Руководство

6. Что такое процедура?
– Правила использования программного и аппаратного обеспечения в компании
– Пошаговая инструкция по выполнению задачи
– Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах
– Обязательные действия

7. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?
– Поддержка высшего руководства
– Эффективные защитные меры и методы их внедрения
– Актуальные и адекватные политики и процедуры безопасности
– Проведение тренингов по безопасности для всех сотрудников

8. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?
– Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски
– Когда риски не могут быть приняты во внимание по политическим соображениям
– Когда необходимые защитные меры слишком сложны
– Когда стоимость контрмер превышает ценность актива и потенциальные потери

9. Что такое политики безопасности?
– Пошаговые инструкции по выполнению задач безопасности
– Общие руководящие требования по достижению определенного уровня безопасности
– Широкие, высокоуровневые заявления руководства
– Детализированные документы по обработке инцидентов безопасности

10. Какая из приведенных техник является самой важной при выборе конкретных защитных мер?
– Анализ рисков
– Анализ затрат / выгоды
– Результаты ALE
– Выявление уязвимостей и угроз, являющихся причиной риска

6.2. Промежуточный контроль *(зачет)*

6.2.1. Перечень вопросов к зачету

1. Основные понятия и определения информационной безопасности. Особенности защиты информации в социально-экономических информационных системах (СЭИС)
2. Основные методы и средства защиты информации, применяемые в корпоративных экономических информационных системах (КЭИС).
3. Правовые меры обеспечения информационной безопасности в социально-экономических информационных системах (СЭИС).
4. Законодательные и нормативные акты Российской Федерации в области защиты информации.
5. Использование электронных ключей для организации информационной безопасности в КЭИС.
6. Организационно-административные методы защиты, применяемые в социально-экономических информационных системах.
7. Формирование политики безопасности предприятия (организации).
8. Идентификация пользователей, аутентификация пользователей и авторизация пользователей (назначение и способы реализации).
9. Криптографические методы защиты информации. Математическое и алгоритмическое обеспечение криптографических методов защиты информации.
10. Симметричные и асимметричные криптосистемы.
11. Электронная цифровая подпись. Использование ЭЦП в экономических системах.
12. Защита информации в компьютерных сетях. Объекты защиты информации в сети.
13. Потенциальные угрозы безопасности в Интранет. Методы защиты информации в Интранет.
14. Потенциальные угрозы безопасности в Интернет (и в частности в электронной коммерции). Методы защиты информации в сети Интернет.
15. Использование межсетевых экранов для обеспечения информационной безопасности в Интернет.
16. Частные виртуальные сети (VPN). Классификация VPN.
17. Количественный подход к информационной безопасности. Оценка защищенности механизмов защиты.
18. Методы защиты от вредоносных программ в СЭИС.
19. Аудит информационной безопасности.
20. Управление информационными рисками.

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

а) основная литература:

	Год издания	Вид (бум., электр.)	Количество экз. (для электронных изданий – эл. адрес)
Издательство "Лань"	2019	электр.	https://e.lanbook.com/book/114688
Издательство "Горячая линия-Телеком"	2018	электр.	https://e.lanbook.com/book/111075
Издательство "Лань"	2020	электр.	https://e.lanbook.com/book/133924

б) дополнительная литература:

Наименование, издательство	Год издания	Вид (бум., электр.)	Количество экз. (для электронных изданий – эл. адрес)
Издательство "ФЛИНТА"	2015	электр.	https://e.lanbook.com/book/62972
Вузовское образование	2018	электр.	http://www.iprbookshop.ru/77320.html
Интернет-Университет Информационных Технологий (ИНТУИТ)	2016	электр.	http://www.iprbookshop.ru/52209.html
Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа	2020	электр.	http://www.iprbookshop.ru/89443.html
Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование	2017	электр.	http://www.iprbookshop.ru/72341.html
Ай Пи Ар Букс	2015	электр.	http://www.iprbookshop.ru/33857.html

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к нескольким электронно-библиотечным системам (электронным библиотекам):

– «Университетская библиотека онлайн» ООО «Директ-Медиа», адрес доступа: www.biblioclub.ru, доступ круглосуточный неограниченный из любой точки Интернет при условии регистрации в БГУ;

– Универсальная справочно-информационная полнотекстовая база данных ООО «ИВИС», адрес доступа: www.ebiblioteka.ru, доступ круглосуточный неограниченный из любой точки Интернет при условии регистрации в БГУ;

– Электронная библиотека Издательского дома «Гребенников», адрес доступа: www.grebennikon.ru; доступ с компьютеров сети БГУ (по IP-адресам)

– Научная электронная библиотека «Киберленинка», адрес доступа: http://cyberleninka.ru, доступ круглосуточный, неограниченный для всех пользователей, бесплатное чтение и скачивание всех научных публикаций, в том числе пакет «Юридические науки», коллекция из 7 журналов по правоведению;

– НЭБ «eLibrary», адрес доступа: www.elibrary.ru, доступ к российским журналам, находящимся полностью или частично в открытом доступе при условии регистрации;

– Информационная система «Единое окно доступа к образовательным ресурсам», поставщик – Федеральное государственное автономное учреждение «Государственный научно-исследовательский институт информационных технологий и телекоммуникаций», адрес доступа: http://window.edu.ru, доступ свободный к интегральному каталогу образовательных Интернет-ресурсов и к электронной библиотеке учебно-методических материалов для общего и профессионального образования, доступ круглосуточный неограниченный для всех пользователей;

– Изд-во «Лань», адрес доступа: http://e.lanbook.com, бесплатный полнотекстовый доступ к 7 коллекциям издательства;

9. Методические указания для обучающихся по освоению дисциплины (модуля)

Изучать дисциплину рекомендуется в соответствии с той последовательностью, которая обозначена в ее содержании.

На лекциях преподаватель озвучивает тему, знакомит с перечнем литературы по теме, обосновывает место и роль этой темы в данной дисциплине, раскрывает ее практическое значение. В ходе лекций обучающемуся необходимо вести конспект, фиксируя основные понятия и проблемные вопросы.

Практические занятия по своему содержанию связаны с тематикой лекционных

занятий. Начинать подготовку к занятию целесообразно с конспекта лекций. Задание на практическое занятие сообщается обучающимся до его проведения.

Изучение дисциплины (модуля) включает самостоятельную работу обучающегося.

Основными видами самостоятельной работы обучающихся с участием преподавателей являются:

- текущие консультации;

Основными видами самостоятельной работы обучающихся без участия преподавателей являются:

- формирование и усвоение содержания конспекта лекций на базе рекомендованной лектором учебной литературы, включая информационные образовательные ресурсы (электронные учебники, электронные библиотеки и др.);
- самостоятельное изучение отдельных тем или вопросов по учебникам или учебным пособиям;
- выполнение домашних заданий в виде решения отдельных задач, проведения типовых расчетов, расчетно-компьютерных и индивидуальных работ по отдельным разделам содержания дисциплин и др.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационно-справочных систем (при *необходимости)*:

В учебном процессе, помимо полного пакета Microsoft Office 2016, используется специализированное программное обеспечение:

7-Zip

Пакет OpenOffice

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю):

- лекционные аудитории;
- аудитории для проведения семинарских и практических занятий;
- мультимедийные аудитории, оборудованные интерактивными досками;

Модуль 4

Методы и средства обеспечения безопасности информационных технологий

1. Цели освоения дисциплины

Целью освоения дисциплины «Методы и средства обеспечения безопасности информационных технологий» является формирование теоретических и практических знаний, умений и навыков, позволяющих осуществлять управление безопасностью информационных технологий, выбор методов и средств ее обеспечения.

2.Место дисциплины в структуре ДПП

Дисциплина «Методы и средства обеспечения безопасности информационных технологий» относится к четвертому разделу (модуль 4) ДПП.

Знания, умения и навыки, полученные в процессе изучения дисциплины «Методы и средства обеспечения безопасности информационных технологий», в дальнейшем используются в процессе самостоятельной исследовательской и практической работе слушателей.

3. Перечень планируемых результатов обучения по дисциплине (модулю) соотнесенных с планируемыми результатами освоения программы

Имеющаяся квалификация и (или) уровень образования (при наличии) соответствующего требования к слушателям:

Виды деятельности	Профессиональные компетенции или трудовые функции	Практический опыт	Умения	Знания
научно-педагогическая деятельность	ПК-18 способен анализировать и выбирать методы и средства обеспечения информационной безопасности	навыками анализа и выбора методов и средств обеспечения информационной безопасности	применить и настроить различные средства защиты информации	методы и средства защиты информации
	ПК-20 способен выбирать необходимые для организации информационные ресурсы и источники знаний в электрон-ной среде	навыками доступа к электронным информационным ресурсам, базам данных, а также библиотекам, архивам	оценивать качество информационных ресурсов	методы применения современных информационных ресурсов в профессиональной деятельности

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 76 часов.

4.1. Содержание разделов дисциплины

Форма обучения заочная (очно-заочная)

№ п/п	Раздел и тема дисциплины	Семестр	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)			Формы текущего контроля успеваемости
			Лекции	Семинар Лаборат. Практич.	Самост. раб.	
1	Технические средства и методы защиты информации	1	2	2	20	Выполнение тестовых заданий
2	Программно-аппаратные средства и методы обеспечения информационной безопасности	1	2	2	22	Выполнение тестовых заданий
3	Криптографические методы защиты информации	1	2	2	22	Выполнение тестовых заданий
	ИТОГО		**6**	**6**	**64**	

4.2. Лекционные занятия, их содержание

№ п/п	Наименование разделов и тем	Содержание
1	Технические средства и методы защиты информации	Инженерная защита объектов. Защита информации от утечки по техническим каналам.
2	Программно-аппаратные средства и методы обеспечения информационной безопасности	Основные виды сетевых и компьютерных угроз. Средства и методы защиты от сетевых компьютерных угроз.
3	Криптографические методы защиты информации	Симметричные и ассиметричные системы шифрования. Цифровые подписи (Электронные подписи). Инфраструктура открытых ключей. Криптографические протоколы.

4.3. Семинарские, практические, лабораторные занятия, их содержание

№ п/п	Наименование разделов и тем	Содержание
1	Использование криптографических средств защиты информации	Создание зашифрованных файлов и криптоконтейнеров и их расшифрование
2	Реализация работы инфраструктуры открытых ключей	Создание удостоверяющего центра, генерация открытых и секретных ключей, создание сертификатов открытых ключей, создание электронной подписи, проверка электронной подписи.
3	Средства стеганографии для защиты информации	Использование средств стеганографии для защиты файлов.

4.4 Вид и форма промежуточной аттестации

Промежуточный контроль проводится в форме зачета.

5. Перечень учебно-методического обеспечения для самостоятельной работы

обучающихся по дисциплине (модулю)

В процессе самостоятельной работы обучающиеся, помимо основной и дополнительной литературы, рекомендованной в п.7, могут пользоваться следующими методическими материалами:

- Практикумы, сборники задач;
- Прочее

6. Оценочные средства для проведения промежуточной аттестации по дисциплине

6.1. Текущий контроль

6.1.1. Образцы тестовых и контрольных заданий текущего контроля

Комплект тестовых заданий

1. Спам распространяет поддельные сообщения от имени банков или финансовых компаний, целью которых является сбор логинов, паролей и пин-кодов пользователей:
   - черный пиар;
   - фишинг;
   - нигерийские письма;
   - источник слухов;
   - пустые письма.

2. Антивирус обеспечивает поиск вирусов в оперативной памяти, на внешних носителях путем подсчета и сравнения с эталоном контрольной суммы:
   - детектор;
   - доктор;
   - сканер;
   - ревизор;
   - сторож.

3. Антивирус не только находит зараженные вирусами файлы, но и "лечит" их, т.е. удаляет из файла тело программы вируса, возвращая файлы в исходное состояние:
   - детектор;
   - доктор;
   - сканер;
   - ревизор;
   - сторож.

4. Антивирус запоминает исходное состояние программ, каталогов и системных областей диска когда компьютер не заражен вирусом, а затем периодически или по команде пользователя сравнивает текущее состояние с исходным:
   - детектор;
   - доктор;
   - сканер;
   - ревизор;
   - сторож.

5. . Антивирус представляет собой небольшую резидентную программу, предназначенную для обнаружения подозрительных действий при работе компьютера, характерных для вирусов:
   - детектор;
   - доктор;
   - сканер;
   - ревизор;
   - сторож.

6. Активный перехват информации это перехват, который:

- заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;
- основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;
- неправомерно использует технологические отходы информационного процесса;
- осуществляется путем использования оптической техники;
- осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

7. Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработки информации называется:
- активный перехват;
- пассивный перехват;
- аудиоперехват;
- видеоперехват;
- просмотр мусора.

8. Перехват, который основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций называется:
- активный перехват;
- пассивный перехват;
- аудиоперехват;
- видеоперехват;
- просмотр мусора.

9. Перехват, который осуществляется путем использования оптической техники называется:
- активный перехват;
- пассивный перехват;
- аудиоперехват;
- видеоперехват;
- просмотр мусора.

10. К внутренним нарушителям информационной безопасности относится:
- клиенты;
- пользователи системы;
- посетители;
- любые лица, находящиеся внутри контролируемой территории;
- представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации.
- персонал, обслуживающий технические средства.
- сотрудники отделов разработки и сопровождения ПО;
- технический персонал, обслуживающий здание

6.2. Промежуточный контроль *(зачет)*

6.2.1. Перечень вопросов к зачету

1. Цели государства в области обеспечения информационной безопасности.
2. Основные нормативные акты РФ, связанные с правовой защитой информации.
3. Виды компьютерных преступлений.
4. Способы и механизмы совершения информационных компьютерных преступлений.
5. Основные параметры и черты информационной компьютерной преступности в России.
6. Компьютерный вирус. Основные виды компьютерных вирусов.
7. Методы защиты от компьютерных вирусов.
8. Типы антивирусных программ.
9. Защиты от несанкционированного доступа. Идентификация и аутентификация пользователя.
10. Основные угрозы компьютерной безопасности при работе в сети Интернет.
11. Виды защищаемой информации.
12. Государственная тайна как особый вид защищаемой информации.
13. Конфиденциальная информация.
14. Система защиты государственной тайны.
15. Правовой режим защиты государственной тайны.
16. Защита интеллектуальной собственности средствами патентного и авторского права.
17. Международное законодательство в области защиты информации.
18. Программно-аппаратные средства обеспечения информационной безопасности в информационных сетях.
19. Симметричные шифры.

20. Ассиметричные шифры.
21. Криптографические протоколы.
22. Криптографические хеш-функции.
23. Электронная подпись.
24. Организационное обеспечение информационной безопасности.
25. Служба безопасности организации.
26. Методы защиты информации от утечки в технических каналах.
27. Инженерная защита и охрана объектов.

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

а) основная литература:

	Год издания	Вид (бум., электр.)	Количество экз. (для электронных изданий – эл. адрес)
Издательство "Лань"	2019	электр.	https://e.lanbook.com/book/114688
Издательство "Горячая линия-Телеком"	2018	электр.	https://e.lanbook.com/book/111075
Издательство "Лань"	2020	электр.	https://e.lanbook.com/book/133924

б) дополнительная литература:

Наименование, издательство	Год издания	Вид (бум., электр.)	Количество экз. (для электронных изданий – эл. адрес)
Издательство "ФЛИНТА"	2015	электр.	https://e.lanbook.com/book/62972
Вузовское образование	2018	электр.	http://www.iprbookshop.ru/77320.html
Интернет-Университет Информационных Технологий (ИНТУИТ)	2016	электр.	http://www.iprbookshop.ru/52209.html
Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа	2020	электр.	http://www.iprbookshop.ru/89443.html
Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование	2017	электр.	http://www.iprbookshop.ru/72341.html
Ай Пи Ар Букс	2015	электр.	http://www.iprbookshop.ru/33857.html

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к нескольким электронно-библиотечным системам (электронным библиотекам):

– «Университетская библиотека онлайн» ООО «Директ-Медиа», адрес доступа: www.biblioclub.ru, доступ круглосуточный неограниченный из любой точки Интернет при условии регистрации в БГУ;

– Универсальная справочно-информационная полнотекстовая база данных ООО «ИВИС», адрес доступа: www.ebiblioteka.ru, доступ круглосуточный неограниченный из любой точки Интернет при условии регистрации в БГУ;

– Электронная библиотека Издательского дома «Гребенников», адрес доступа: www.grebennikon.ru; доступ с компьютеров сети БГУ (по IP-адресам)

– Научная электронная библиотека «Киберленинка», адрес доступа: http://cyberleninka.ru, доступ круглосуточный, неограниченный для всех пользователей, бесплатное чтение и скачивание всех научных публикаций, в том числе пакет «Юридические науки», коллекция из 7 журналов по правоведению;

– НЭБ «eLibrary», адрес доступа: www.elibrary.ru, доступ к российским журналам, находящимся полностью или частично в открытом доступе при условии регистрации;

– Информационная система «Единое окно доступа к образовательным ресурсам», поставщик – Федеральное государственное автономное учреждение «Государственный

научно-исследовательский институт информационных технологий и телекоммуникаций», адрес доступа: http://window.edu.ru, доступ свободный к интегральному каталогу образовательных Интернет-ресурсов и к электронной библиотеке учебно-методических материалов для общего и профессионального образования, доступ круглосуточный неограниченный для всех пользователей;

– Изд-во «Лань», адрес доступа: http://e.lanbook.com, бесплатный полнотекстовый доступ к 7 коллекциям издательства;

9. Методические указания для обучающихся по освоению дисциплины (модуля)

Изучать дисциплину рекомендуется в соответствии с той последовательностью, которая обозначена в ее содержании.

На лекциях преподаватель озвучивает тему, знакомит с перечнем литературы по теме, обосновывает место и роль этой темы в данной дисциплине, раскрывает ее практическое значение. В ходе лекций обучающемуся необходимо вести конспект, фиксируя основные понятия и проблемные вопросы.

Практические занятия по своему содержанию связаны с тематикой лекционных занятий. Начинать подготовку к занятию целесообразно с конспекта лекций. Задание на практическое занятие сообщается обучающимся до его проведения.

Изучение дисциплины (модуля) включает самостоятельную работу обучающегося.

Основными видами самостоятельной работы обучающихся с участием преподавателей являются:

- текущие консультации;

Основными видами самостоятельной работы обучающихся без участия преподавателей являются:

- формирование и усвоение содержания конспекта лекций на базе рекомендованной лектором учебной литературы, включая информационные образовательные ресурсы (электронные учебники, электронные библиотеки и др.);
- самостоятельное изучение отдельных тем или вопросов по учебникам или учебным пособиям;
- выполнение домашних заданий в виде решения отдельных задач, проведения типовых расчетов, расчетно-компьютерных и индивидуальных работ по отдельным разделам содержания дисциплин и др.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационно-справочных систем (при *необходимости)*:

В учебном процессе, помимо полного пакета Microsoft Office 2016, используется специализированное программное обеспечение:

7-Zip
Пакет OpenOffice

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю):

- лекционные аудитории;
- аудитории для проведения семинарских и практических занятий;
- мультимедийные аудитории, оборудованные интерактивными досками;