

**«Федеральное государственное бюджетное образовательное
учреждение высшего образования
«РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА
И ГОСУДАРСТВЕННОЙ СЛУЖБЫ
ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»**

**Институт права и национальной безопасности
КАФЕДРА социально-гуманитарных, экономических и
естественно-научных дисциплин**

УТВЕРЖДЕНА
решением кафедры социально-гуманитарных,
экономических
и естественно-научных дисциплин
Протокол от « 13 » мая 2019 г. № 10_

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

К.М.07.ДВ.03.01 Информационно-технологическая безопасность

(индекс, наименование дисциплины (модуля), в соответствии с учебным планом)

направление подготовки (специальность)

38.03.04 Государственное и муниципальное управление

(код, наименование направления подготовки (специальности))

Безопасность сферы предоставления государственных и муниципальных услуг

(направленность(и) (профиль (и)/специализация(ии))

Бакалавр

(квалификация)

Очная

(форма(ы) обучения)

Год набора-2019

Москва, 2019г.

Автор(ы)-составитель(и):

Кандидат технических наук, доцент _____ Выжигин Александр Юрьевич.

(ученая степень и(или) ученое звание, должность)
(подпись) (Ф.И.О.)

(наименование кафедры)

Заведующий кафедрой

социально-гуманитарных, экономических

и естественно-научных дисциплин к.т.н., доцент

(

_____ Выжигин А.Ю..

СОДЕРЖАНИЕ

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ПРОГРАММЫ.....	4
2. ОБЪЕМ И МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОП ВО.....	5
3. СОДЕРЖАНИЕ И СТРУКТУРА ДИСЦИПЛИНЫ (МОДУЛЯ)	7
4. МАТЕРИАЛЫ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ ОБУЧАЮЩИХСЯ И ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ	10
4.1. ФОРМЫ И МЕТОДЫ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ.....	10
4.2. МАТЕРИАЛЫ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ.....	10
4.3. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ.....	11
4.4. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ	14
5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)	16
6. УЧЕБНАЯ ЛИТЕРАТУРА И РЕСУРСЫ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ "ИНТЕРНЕТ", ВКЛЮЧАЯ ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ).....	18
6.1. ОСНОВНАЯ ЛИТЕРАТУРА.....	18
6.2. ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА.	19
6.3. НОРМАТИВНЫЕ ПРАВОВЫЕ ДОКУМЕНТЫ.	19
6.4. ИНТЕРНЕТ-РЕСУРСЫ.	19
7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ	20

....

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

1.1. Дисциплина **К.М.07.ДВ.03.01 «Информационно-технологическая безопасность»** обеспечивает овладение следующими компетенциями с учетом этапа:

Код компетенции и	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ПК-24	владение технологиями, приемами, обеспечивающими оказание государственных и муниципальных услуг физическим и юридическим лицам	ПК-24.2	способность по организации предоставления государственных и муниципальных услуг физическим и юридическим лицам в электронной форме.
ПК-26	владением навыками сбора, обработки информации и участия в информатизации деятельности соответствующих органов власти и организаций	ПК-26.2	способность использовать информационно-коммуникационные технологии в профессиональной деятельности, а также участия в информатизации деятельности соответствующих органов власти и организаций.

1.2. В результате освоения дисциплины у студентов должны быть сформированы:

Профессиональные действия	Код этапа освоения компетенции	Результаты обучения
	ПК-24.2	<p>уметь:</p> <ul style="list-style-type: none"> использования информационных баз данных, электронных библиотек и ресурсов для решения профессиональных задач в рамках оказания государственных и муниципальных услуг физическим и юридическим лицам. <p>Владеть навыками:</p> <ul style="list-style-type: none"> анализа, организации и планирования в области предоставления государственных и муниципальных услуг физическим и юридическим лицам; оценки информационных угроз системе предоставления оказания государственных и муниципальных услуг; организации предоставления государственных и муниципальных услуг

		физическим и юридическим лицам в электронной форме; • защиты персональных данных при оказании государственных и муниципальных услуг.
	ПК-26.2	Уметь - определять актуальные угрозы безопасности информации; Владеть навыками • использования информационно-коммуникационных технологий для интенсификации процесса получения, обработки и оценки информации в рамках решения различных задач профессиональной деятельности. • обеспечивать цикл управления с помощью средств ИКТ; • использования информационно-коммуникационных технологий для повышения эффективности деятельности организации.

2. Объем и место дисциплины (модуля) в структуре ОП ВО

Объем дисциплины

Общая трудоемкость дисциплины составляет 2 з.е. (72 а.ч.).

Количество академических часов, выделенных на контактную работу с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся:

- очная форма обучения: лекции – 16 а.ч., практические занятия – 16 а.ч., самостоятельная работа – 40 ч.

Место дисциплины в структуре ОП ВО

Дисциплина относится к комплексным модулям и в соответствии с учебным планом осваивается в 8-м семестре 4 курса очной формы обучения.

Дисциплина является естественно-научной дисциплиной. Ее изучение должно способствовать повышению уровня подготовки будущих специалистов, выработке самостоятельного мышления, умения грамотно и оперативно принимать управленческие решения.

Предшествующими дисциплинами являются:

- Информационная безопасность деятельности государственных и муниципальных служащих
- Основы безопасности в сфере предоставления государственных и муниципальных услуг
- Безопасность информационного общества//Безопасность сетевого общества
- Безопасность общественных связей//Безопасность персональных данных в сфере предоставления государственных муниципальных услуг

Форма промежуточной аттестации в соответствии с учебным планом – 8 семестр – зачет.

3. Содержание и структура дисциплины (модуля)

Таблица 1.

№ п/п	Наименование тем (разделов)	Объем дисциплины, час.						Форма текущего контроля успеваемости*, промежуточной аттестации
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СР	
			Л	ЛР	ПЗ	КСР		
Очная форма обучения								
Тема 1	Информационная безопасность в системе национальной безопасности Российской Федерации	18	4		4		10	Устное собеседование
Тема 2	Национальные интересы и угрозы информационной безопасности Российской Федерации в информационной сфере и их обеспечение.	18	4		4		10	Письменный опрос
Тема 3	Основные виды формальных моделей безопасности	18	4		4		10	Устное собеседование
Тема 4	Основные критерии защищенности КС	18	4		4		10	Письменный опрос
	Всего, 8 семестр, Зачет	108	16	0	16		40	

Формы текущего контроля: Устное собеседование, Письменный опрос

Содержание дисциплины (модуля)

№ Раздела	Наименование раздела	Содержание раздела
-----------	----------------------	--------------------

1	Информационная безопасность в системе национальной безопасности Российской Федерации	<p>Задачи и программа курса. Понятие национальной безопасности. Виды безопасности и сферы жизнедеятельности личности, общества и государства: экономическая, внутривластная, социальная, международная, информационная, военная, пограничная, экологическая и другие. Виды защищаемой информации. Основные понятия и общеметодологические принципы теории информационной безопасности. Роль информационной безопасности в обеспечении национальной безопасности государства.</p>
2	Национальные интересы и угрозы информационной безопасности Российской Федерации в информационной сфере и их обеспечение.	<p>Интересы личности в информационной сфере. Интересы общества в информационной сфере. Интересы государства в информационной сфере. Основные составляющие национальных интересов Российской Федерации в информационной сфере.</p> <p>Угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России.</p> <p>Угрозы информационному обеспечению государственной политики Российской Федерации. Угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходе этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов.</p> <p>Угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.</p> <p>Внешние источники угроз. Внутренние источники угроз. Направления обеспечения информационной безопасности государства. Проблемы региональной информационной безопасности.</p>

		Основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации.
3	Основные виды формальных моделей безопасности	Модели систем дискреционного управления доступом. Модели изолированной программной среды (ИПС). Модели систем мандатного управления доступом. Модели безопасности информационных потоков. Модели ролевого управления доступом.
4	Основные критерии защищенности КС	Руководящие документы ФСТЭК России. Критерии и классы защищенности средств вычислительной техники и КС от несанкционированного доступа (НСД) к информации. Общие критерии.

Лабораторные работы (ЛБ)
Не предусмотрены.

Практические занятия (ПР)

№ п/п	№ раздела дисциплины	Тематика практических занятий	Трудоемкость (в акад. час.)
1	1	Понятие национальной безопасности. Роль информационной безопасности в обеспечении национальной безопасности государства.	4
2	2	Основные составляющие национальных интересов Российской Федерации в информационной сфере и их содержание. Угрозы информационной безопасности. Источники угроз.	4
3			
4			
5	3	Модели систем дискреционного и мандатного управления доступом. Модели систем ролевого управления доступом и информационными потоками.	4
6			
7	4	Руководящие документы ФСТЭК России. Критерии и классы защищенности средств вычислительной техники и КС от несанкционированного доступа (НСД) к информации. Общие критерии.	4
8	4		

<i>Всего в 8 семестре:</i>	<i>16</i>
Всего:	16

4. Материалы текущего контроля успеваемости обучающихся и фонд оценочных средств промежуточной аттестации по дисциплине

4.1. Формы и методы текущего контроля успеваемости и промежуточной аттестации.

4.1.1. В ходе реализации дисциплины **К.М.07.ДВ.03.01 Информационно-технологическая безопасность** используются следующие методы текущего контроля успеваемости обучающихся:

- при проведении занятий лекционного типа: опрос (тестирование и домашняя работа)
- при проведении практических занятий: опрос, тестирование, контрольная работа.

4.1.2. Промежуточная аттестация проводится в форме:

зачёт (8 семестр) – при проведении занятий лекционного типа тестирование; при проведении занятий семинарского типа - аудиторные проверочные работы; при контроле результатов самостоятельной работы студентов - домашние проверочные работы.

4.2. Материалы текущего контроля успеваемости.

Вопросы для самостоятельной подготовки по темам дисциплины

Раздел 1.

1. Виды безопасности и сферы жизнедеятельности личности, общества и государства
2. Виды защищаемой информации
3. Основные понятия и общеметодологические принципы теории информационной безопасности
4. Роль информационной безопасности в обеспечении национальной безопасности государства

Раздел 2.

1. Интересы личности в информационной сфере
2. Интересы общества в информационной сфере
3. Интересы государства в информационной сфере
4. Основные составляющие национальных интересов Российской Федерации в информационной сфере
5. Угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности
6. Угрозы информационному обеспечению государственной политики Российской Федерации

7. Угрозы развитию отечественной индустрии информации
8. Угрозы безопасности информационных и телекоммуникационных средств и систем
9. Внешние источники угроз
10. Внутренние источники угроз
11. Направления обеспечения информационной безопасности государства
12. Проблемы региональной информационной безопасности
13. Основные средства и способы обеспечения информационной безопасности
14. Принципы построения систем защиты информации

Раздел 3.

1. Модели систем дискреционного управления доступом
2. Модели изолированной программной среды (ИПС)
3. Модели систем мандатного управления доступом
4. Исследование системы ZABVIX
5. Модели безопасности информационных потоков
6. Модели ролевого управления доступом

Раздел 4.

1. Руководящие документы ФСТЭК России
2. Критерии и классы защищенности средств вычислительной техники от несанкционированного доступа (НСД) к информации
3. Критерии и классы защищенности средств КС от несанкционированного доступа (НСД) к информации

4.3. Оценочные средства для промежуточной аттестации.

4.3.1. Формируемые компетенции

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ПК-24	владение технологиями, приемами, обеспечивающими оказание государственных и муниципальных услуг физическим и юридическим лицам	ПК-24.2	способность по организации предоставления государственных и муниципальных услуг физическим и юридическим лицам в электронной форме.
ПК-26	владением навыками сбора, обработки информации и участия в информатизации	ПК – 26.2	Знать - классификацию угроз информационной безопасности;

	деятельности соответствующих органов власти и организаций		Уметь - определять актуальные угрозы безопасности информации; Владеть -навыками составления модели нарушителей безопасности информации
--	---	--	---

Этап освоения компетенции	Показатель оценивания	Критерий оценивания	Рекомендуемые средства (методы) оценивания
ПК-24.2 способность по организации предоставления государственных и муниципальных услуг физическим и юридическим лицам в электронной форме.	Знает основы законодательного и нормативно-правового обеспечения системы предоставления электронных государственных и муниципальных услуг физическим и юридическим лицам ¹ . Самостоятельно использует технологии при организации предоставления государственных и муниципальных услуг физическим и юридическим лицам в электронной форме. Обладает навыками пользования основными электронными документами и	Продемонстрировано знание основ законодательного и нормативно-правового обеспечения системы предоставления электронных государственных и муниципальных услуг физическим и юридическим лицам. Корректно использует технологии при организации предоставления государственных и муниципальных услуг физическим и юридическим лицам в электронной форме. Демонстрирует навыки пользования основными электронными документами и идентификационными инструментами для граждан из приложений «Электронного правительства».	Устное собеседование Защита презентаций Ситуационные задачи

¹ В частности, Постановление Правительства РФ от 08.06.2011г. № 451 «Об инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме» и Постановление Правительства РФ от 24.10.2011г. № 861 «О федеральных государственных информационных системах, обеспечивающих предоставление в электронной форме государственных и муниципальных услуг (осуществление функций)».

	идентификационным и инструментами для граждан в приложениях «Электронного правительства».		
ПК-26.2 способность использовать информационно-коммуникационные технологии в профессиональной деятельности, а также участия в информатизации деятельности соответствующих органов власти и организаций.	Самостоятельно использует информационно-коммуникационные технологии для интенсификации процесса получения, обработки и оценки информации для решения задач в рамках профессиональной деятельности, а также участия в информатизации деятельности соответствующих органов власти и организаций. Обладает навыками пользования информационными базами данных, электронными библиотеками и ресурсами.	Корректно использует информационно-коммуникационные технологии для интенсификации процесса получения, обработки и оценки информации для решения задач в рамках профессиональной деятельности, а также участия в информатизации деятельности соответствующих органов власти и организаций. Демонстрирует навыки пользования информационными базами данных, электронными библиотеками и ресурсами.	Ситуационные задачи Защита презентаций

4.3.2 Типовые оценочные средства

Перечень вопросов для подготовки к промежуточной аттестации (зачет, 8 семестр)

1. Виды безопасности и сферы жизнедеятельности личности, общества и государства
2. Виды защищаемой информации
3. Основные понятия и общеметодологические принципы теории информационной безопасности
4. Роль информационной безопасности в обеспечении национальной безопасности государства
5. Интересы личности в информационной сфере
6. Интересы общества в информационной сфере

7. Интересы государства в информационной сфере
8. Основные составляющие национальных интересов Российской Федерации в информационной сфере
9. Угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности
10. Угрозы информационному обеспечению государственной политики Российской Федерации
11. Угрозы развитию отечественной индустрии информации
12. Угрозы безопасности информационных и телекоммуникационных средств и систем
13. Внешние источники угроз
14. Внутренние источники угроз
15. Направления обеспечения информационной безопасности государства
16. Проблемы региональной информационной безопасности
17. Основные средства и способы обеспечения информационной безопасности
18. Принципы построения систем защиты информации
19. Модели систем дискреционного управления доступом
20. Модели изолированной программной среды (ИПС)
21. Модели систем мандатного управления доступом
22. Система ZABBIX
23. Модели безопасности информационных потоков
24. Модели ролевого управления доступом
25. Руководящие документы ФСТЭК России
26. Критерии и классы защищенности средств вычислительной техники от несанкционированного доступа (НСД) к информации
27. Критерии и классы защищенности средств КС от несанкционированного доступа (НСД) к информации

К зачету допускаются студенты, выполнившие все требования учебной программы, выполнившие в установленные сроки все виды заданий и работ, не имеющим задолженностей по итогам текущего контроля успеваемости.

Подготовка к зачету предусматривает устное повторение пройденного учебного материала по дисциплине (с использованием конспектов, учебных пособий, дополнительной литературы, выполненных работ и заданий).

4.4. Методические материалы

Для контроля усвоения данной дисциплины учебным планом предусмотрены аудиторские работы (8 семестр), зачет.

Шкала оценивания:

«Зачет» – выставляется, если сформированность заявленных дескрипторов компетенций на 50% и более оценивается не ниже «удовлетворительно» при условии отсутствия критерия «неудовлетворительно». Выставляется, когда обучающийся показывает хорошие знания изученного учебного материала; самостоятельно, логично и последовательно

излагает, и интерпретирует материалы учебного курса; полностью раскрывает смысл предлагаемого вопроса; владеет основными терминами и понятиями изученного курса; показывает умение переложить теоретические знания на предполагаемый практический опыт.

«Незачет» – выставляется, если сформированность заявленных дескрипторов компетенций менее чем 50% (в соответствии с картами компетенций ОПОП) оценивается критериями «удовлетворительно», «хорошо» и «отлично»: при ответе обучающегося выявились существенные пробелы в знаниях основных положений фактического материала, неумение с помощью преподавателя получить правильное решение конкретной практической задачи из числа предусмотренных рабочей программой учебной дисциплины.

Оценивание обучающегося на зачете по дисциплине

Таблица 2.

Баллы рейтингово й оценки	Оценка экзамена (стандартная)	Требования к знаниям
90-100	5, отлично / зачтено	<p><i>Оценка «отлично»</i> выставляется обучающемуся, если он:</p> <p>Применяет в своей работе информационные и библиографические данные; способен применять в своей профессиональной деятельности в полном объеме полученную информацию</p> <p>Самостоятельно, без затруднений применяет информационно-коммуникационные технологии в своей деятельности; пояснить связь представленной информации с основами профессиональной деятельности; способен сформулировать предложения по ее совершенствованию</p> <p>осуществляет решение стандартных задач профессиональной деятельности с учетом основных требований информационной безопасности; способен выявить проблемные аспекты и объяснить их; дает рекомендации по устранению выявленных ошибок</p>
75-89	4, хорошо / зачтено	<p><i>Оценка «хорошо»</i> выставляется обучающемуся, если он:</p> <p>Применяет в своей работе информационные данные; не допускает ошибки и неточности;</p> <p>Самостоятельно, без затруднений применяет информационно-коммуникационные технологии в своей деятельности; при самостоятельной работе способен обосновать свои действия.</p> <p>Самостоятельно осуществляет решение стандартных задач профессиональной деятельности с учетом основных требований информационной безопасности;</p>

55-74	3, удовлетворительно / зачтено	<p><i>Оценка «удовлетворительно»</i> выставляется обучающемуся, если он:</p> <p>Применяет в своей работе информационные и библиографические данные; допускает негрубые ошибки и неточности.</p> <p>Самостоятельно применяет информационно-коммуникационные технологии в своей деятельности; при самостоятельной работе допускает негрубые ошибки</p> <p>Самостоятельно осуществляет решение стандартных задач профессиональной деятельности с учетом основных требований информационной безопасности</p>
0-5	2, Неудовлетворительно / не зачтено	<p><i>Оценка «неудовлетворительно»</i> выставляется обучающемуся, который:</p> <p>Применяет в своей работе информационные и библиографические данные; допускает грубые ошибки и неточности.</p> <p>С помощью преподавателя применяет информационно-коммуникационные технологии в своей деятельности; при самостоятельной работе допускает грубые ошибки</p> <p>Осуществляет решение стандартных задач профессиональной деятельности с учетом основных требований информационной безопасности, пользуясь помощью преподавателя</p>

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

Цель методических рекомендаций - обеспечить студенту оптимальную организацию процесса изучения дисциплины, а также выполнения различных форм самостоятельной работы.

Студентам необходимо ознакомиться: с содержанием рабочей программы дисциплины, с целями и задачами дисциплины, ее связями с другими дисциплинами образовательной программы, методическими разработками по данной дисциплине, имеющимся на образовательном портале и сайте кафедры, с графиком консультаций преподавателей кафедры.

Рекомендации по подготовке к лекционным занятиям (теоретический курс).

Изучение дисциплины требует систематического и последовательного накопления знаний, следовательно, пропуски отдельных тем не позволяют глубоко освоить предмет. Именно поэтому контроль над систематической работой студентов всегда находится в центре внимания кафедры.

Студентам необходимо:

- перед каждой лекцией просматривать рабочую программу дисциплины, что позволит сэкономить время на записывание темы лекции, ее основных вопросов, рекомендуемой литературы;
- на отдельные лекции приносить соответствующий материал на бумажных носителях, представленный лектором на портале или присланный на «электронный почтовый ящик группы» (таблицы, графики, схемы, презентации). Данный материал будет охарактеризован, прокомментирован, дополнен непосредственно на лекции;

- перед очередной лекцией необходимо просмотреть по конспекту материал предыдущей лекции. При затруднениях в восприятии материала следует обратиться к основным литературным источникам. Если разобраться в материале опять не удалось, то обратитесь к лектору (по графику его консультаций) или к преподавателю на практических занятиях.

Рекомендации по подготовке к практическим (семинарским, лабораторным) занятиям.

Студентам следует:

- приносить с собой рекомендованную преподавателем литературу к конкретному занятию;
- до очередного практического занятия по рекомендованным литературным источникам проработать теоретический и практический материал, соответствующей темы занятия и отработать задания, определённые для подготовки к практическому занятию;
- при подготовке к практическим занятиям следует обязательно использовать не только лекции, учебную литературу, но и нормативно-правовые акты и материалы правоприменительной практики;
- теоретический материал следует соотносить с правовыми нормами, так как в них могут быть внесены изменения, дополнения, которые не всегда отражены в учебной литературе;
- в начале занятий задать преподавателю вопросы по материалу, вызвавшему затруднения в его понимании и освоении при решении задач, заданных для самостоятельного решения;
- в ходе практического занятия давать конкретные, четкие ответы по существу вопросов;
- на занятии доводить каждую задачу до окончательного решения, демонстрировать понимание проведенных расчетов (анализов, ситуаций), в случае затруднений обращаться к преподавателю.

Методические рекомендации по подготовке, написанию и оформлению контрольной работы

Выполнение контрольной работы проводится по теме 1 с целью формирования общепрофессиональных компетенций и способностей к научно-исследовательской работе, позволяющих:

- осуществлять поиск и использование информации (в том числе справочной, нормативной и правовой), обработку данных с применением современных информационных технологий, необходимых для решения профессиональных задач;
 - выбирать инструментальные средства для обработки данных в соответствии с поставленной задачей, применяя современный математический и статистический аппарат, программные продукты;
 - анализировать результаты, обосновывать полученные выводы.
- Контрольные работы должны быть выполнены в полном объеме.
Контрольная работа должна содержать:
Задание, решение и ответ каждой задачи работы;

Методические рекомендации по выполнению различных форм самостоятельных домашних заданий.

Самостоятельная работа студентов включает в себя выполнение различного рода заданий, которые ориентированы на более глубокое усвоение материала изучаемой дисциплины. По каждой теме учебной дисциплины студентам предлагается перечень практических заданий для самостоятельной работы, определяемый преподавателем в ходе выполняемости практических и лабораторных работ с применением компьютерной техники.

К выполнению заданий для самостоятельной работы предъявляются следующие требования: задания должны выполняться самостоятельно и представляться в установленный срок.

Методические рекомендации по работе с литературой.

Любая форма самостоятельной работы студента (подготовка к семинарскому занятию, написание эссе, контрольной работы, доклада и т.п.) начинается с изучения соответствующей литературы как в библиотеке, так и дома.

К каждой теме учебной дисциплины подобрана основная и дополнительная литература.

Основная литература - это учебники и учебные пособия.

Дополнительная литература - это монографии, сборники научных трудов, журнальные и газетные статьи, различные справочники, энциклопедии, интернет ресурсы.

Рекомендации студенту:

- выбранную монографию или статью целесообразно внимательно просмотреть. В книгах следует ознакомиться с оглавлением и научно-справочным аппаратом, прочитать аннотацию и предисловие. Целесообразно ее пролистать, рассмотреть иллюстрации, таблицы, диаграммы, приложения. Такое поверхностное ознакомление позволит узнать, какие главы следует читать внимательно, а какие прочитать быстро;

- в книге или журнале, принадлежащие самому студенту, ключевые позиции можно выделять маркером или делать пометки на полях. При работе с Интернет-источником целесообразно также выделять важную информацию;

- если книга или журнал не являются собственностью студента, то целесообразно записывать номера страниц, которые привлекли внимание. Позже следует возвратиться к ним, перечитать или переписать нужную информацию. Физическое действие по записыванию помогает прочно заложить данную информацию в «банк памяти».

Выделяются следующие виды записей при работе с литературой:

Конспект - краткая схематическая запись основного содержания научной работы. Целью является не переписывание произведения, а выявление его логики, системы доказательств, основных выводов. Хороший конспект должен сочетать полноту изложения с краткостью.

Цитата - точное воспроизведение текста. Заключается в кавычки. Точно указывается страница источника.

Тезисы - концентрированное изложение основных положений прочитанного материала.

Аннотация - очень краткое изложение содержания прочитанной работы.

Резюме - наиболее общие выводы и положения работы, ее концептуальные итоги. Записи в той или иной форме не только способствуют пониманию и усвоению изучаемого материала, но и помогают вырабатывать навыки ясного изложения в письменной форме тех или иных теоретических вопросов.

6. Учебная литература и ресурсы информационно-телекоммуникационной сети "Интернет", включая перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

6.1. Основная литература.

1. Основы информационной безопасности. Белов Е.Б.; **Лось В.П.**; Мещеряков Р.В.; Шелупанов А.А.. Москва: Горячая линия - Телеком Language: Russian, База данных: IPRbooks
2. Основы информационной безопасности. Галатенко В. А.. 01/01/2016 Language: Russian, База данных: Lan Publishing

3. Правовые основы информационной безопасности : учебное пособие. Кожуханов Н. М.; Недосекова Е. С.. РТА, 2013. Language: Russian, База данных: Lan Publishing

6.2. Дополнительная литература.

1. . **Основы информационной безопасности** : [практическое пособие] / А.Н. Калинин, О.К. Синчугов, А.Л. Тележко. - М. : Национальная компьютерная корпорация, 2005. - 159 с. - Библиогр. в конце разделов. - ISBN 5-98597-041-8.
2. Правовые **основы** обеспечения **информационной безопасности** Российской Федерации : учебное пособие / Е.Н. Яковец. - М. : Юрлитинформ, 2010. - 332 с. - Библиогр.: с. 279-316. - ISBN 978-5-93295-645-8.
3. **Основы информационной безопасности** : учебное пособие для вузов : рекомендовано УМО в области прикладной информатики... по специальности "Прикладная информатика" / В.А. Галатенко. - 4-е издание. - М. : Интернет-Университет Информационных Технологий : БИНОМ. Лаборатория знаний, 2012. - 205 с. - (**Основы** информационных технологий). - Библиогр.: с. 200-205. - ISBN 978-5-94774-821-5.

Основы информационной безопасности : учебное пособие : гриф УМО / С.П. Расторгуев. - М. : Академия, 2007. - 192 с. - ISBN 978-5-7695-3098-2.

6.3. Нормативные правовые документы.

1. Доктрина информационной безопасности Российской Федерации.
2. Федеральный закон Российской Федерации «Об информации, информационных технологиях и защите информации» №149-ФЗ от 27 июля 2006 года.
3. Федеральный закон от 4 июля 1996 г. «Об участии в международном информационном обмене».
4. ГОСТ 34.601-90. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания.
5. ГОСТ Р ИСО/МЭК 12207. Процессы жизненного цикла программных средств.

6.4. Интернет-ресурсы.

1. Электронно-библиотечная система «Национальный цифровой ресурс "РУКОНТ"»: <http://rucont.ru/>
2. Справочная правовая система «КонсультантПлюс»: <http://www.consultant.ru/>
3. Справочная правовая система «Гарант»: <http://www.garant.ru>
4. Электронно-библиотечная система «Лань»: <https://e.lanbook.com/>
5. База данных Scopus компании Elsevier B.V.: <https://www.scopus.com/home.uri>
6. База данных Web of Science компании Thomson Reuters (Scientific) LLC.: <http://apps.webofknowledge.com/>
7. Электронные версии научных периодических изданий НЭБ eLIBRARY.RU: elibrary.ru/

7. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

- 1) Специализированные залы для проведения лекций и аудитории для проведения семинарских и практических занятий с использованием мультимедийного оборудования и возможностью прямого выхода в сеть Интернет.
- 2) Специализированная мебель и оргсредства: аудитории и компьютерные классы, оборудованные посадочными местами.
- 3) Технические средства обучения: Персональные компьютеры; компьютерные проекторы; звуковые динамики; программные средства, обеспечивающие просмотр видеофайлов в форматах AVI, MPEG-4, DivX, RMVB, WMV.
- 4) Лицензионные электронные ресурсы: Windows, Microsoft Office (Excel, InfoPath, PowerPoint, Publisher, Word, Access).
- 5) Свободно распространяемое программное обеспечение: PascalABC, PascalABC.NET,
- 6) Информационные справочные и поисковые системы «Консультант Плюс», «Гарант».