Федеральное государственное бюджетное образовательное
учреждение высшего образования
«РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО
ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ
РОССИЙСКОЙ ФЕДЕРАЦИИ»
Среднерусский институт управления - филиал

Щеголев Александр Владимирович

Подписан: Щеголев Александр Владимирович
DN: C=RU, S=Орловская область, T=исполняющий обязанности директора, OU="СРЕДНЕРУССКИЙ ИНСТИТУТ УПРАВЛЕНИЯ - ФИЛИАЛ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ ""РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ"", O="ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ ""РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ"", СНИЛС=13950729986, ИНН=575208091607, E=it@orel.ranepa.ru, G=Александр Владимирович, SN=Щеголев, CN=Щеголев Александр Владимирович
Основание: я подтверждаю этот документ своей удостоверяющей подписью
Местоположение: Среднерусский институт управления

УТВЕРЖДЕНО
Директор Среднерусского института
управления – филиала РАНХиГС
Меркулов П.А.

ПРОГРАММА СПЕЦИАЛИТЕТА

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ,
реализуемой без применения электронного (онлайн) курса

Б1.В.02.05 Правовое обеспечение информационной безопасности

специальность 40.05.01 «Правовое обеспечение национальной безопасности»
специализация: «Уголовно-правовая»
форма обучения: очная, заочная
год набора: 2024

Орел - 2023 г

Автор(ы)-составитель(и) РПД:

Тихалева Е.Ю., кандидат юридических наук, доцент, доцент кафедры

И.о. заведующего кафедрой:

Малявкина Н.В., кандидат юридических наук, доцент, и.о. зав. кафедрой

Рабочая программа дисциплины Б1.В.02.05 Правовое обеспечение информационной безопасности одобрена на заседании кафедры «Конституционное, административное и уголовное право»

Протокол № 1 от 01.09.2023 г.

СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы 4

2. Объем и место дисциплины (модуля) в структуре образовательной программы.....5

3. Содержание и структура дисциплины (модуля).....6

4. Типы оценочных материалов, показатели и критериоценивания.....12

5. Формы аттестации, типовые оценочные материалы для текущего контроля успеваемости обучающихся, критерии и шкалы оценивания.....16

6. Формы промежуточной аттестации, критерии и шкала оценивания, типовые оценочные материалы по дисциплине.....18

7. Методические материалы по освоению дисциплины (модуля) 21

8. Учебная литература и ресурсы информационно-телекоммуникационной сети Интернет 25

9. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы 27

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Дисциплина Б1.В.02.05 Правовое обеспечение информационной безопасности обеспечивает формирование у обучающихся следующих профессиональных компетенций:

ОТФ/ТФ и реквизиты ПС *(при наличии)*	**Кодкомпетенции**	**Наименование компетенции**	**Кодиндикаторадостижениякомпетенций**	**Наименованиеиндикаторадостижениякомпетенций**	**Образовательный результат**
А/02.7 Выполнение отдельных функций процессуального контроля Профессиональный стандарт **09.001** Следователь-криминалист Утвержден приказом Министерства труда и социальной защиты Российской Федерации от 23.03.2015 № 183н	ПКрОС-1	Способен обеспечивать безопасность личности, общества, государства правовыми средствами	ПКрОС-1.1	Использует правовые средства для обеспечения безопасности личности, общества, государства	*ПКр ОС-1.1. З-1.* ***Знает*** объекты безопасности личности, общества, государства, их жизненно важные интересы. *ПКр ОС-1.1. У-1.* ***Умеет***прогнозировать, выявлять, анализировать и оценивать угрозы и риски безопасности личности, общества, государства; *ПКр ОС-1.1. У-2.* ***Умеет***обеспечивать безопасность при принимать правовые меры по нейтрализации угроз безопасности личности, общества, государства.

2. Объем и место дисциплины (модуля) в структуре образовательной программы

Общий объем дисциплины:

3з.е., 108 ак.час.

По очной форме обучения контактная работа обучающихся с преподавателем по видам учебных занятий: 48ак. час на контактную работу с преподавателем, из них 24ак.час на лекции и 24ак.час на практические занятия. 60ак. час на самостоятельную работу обучающихся.

По заочной форме обучения контактная работа обучающихся с преподавателем по видам учебных занятий: 14ак. час на контактную работу с преподавателем, из них 6ак.час на лекции и 8ак.час на практические занятия. 90ак. час на самостоятельную работу обучающихся.

Б1.В.02.05Правовое обеспечение информационной безопасности на 7-м семестре 4-го курса (очная форма обучения) или на 10-м семестре 5-го курса (заочная форма обучения) после изучения дисциплин:

- Б1.О.13 Криминология
- Б1.О.17 Уголовное право
- Б1.О.20 Уголовно-процессуальное право
- Б1. В.02 Обеспечение национальной безопасности;
- Б1.В.03 Уголовно-исполнительное право.

3. Содержание и структура дисциплины (модуля)

3.1. Структура дисциплины (модуля)

Очная форма обучения

№ п/п	Наименование тем и (или) разделов		Объемдисциплины, ак.час											Форма текущего контроля успеваемости, промежуточной аттестации
		ВСЕГО	Контактная работа обучающихся с преподавателем по видам учебных занятий						Периодпромежуточнойаттестации (сессия)			Самостоятельнаяработа		
			Периодтеоретическогообучения											
			Занятиялекционноготипа		Занятиясеминарскоготипа		ИК	КСР	КЭ	Кат тэк	Контроль	СРкр	СРэк	СР
			Л	ВЛ	ЛР	ПЗ								
Тема 1.	Информационная безопасность РоссийскойФедерации и задачи по ее обеспечению	24	6	0	0	6	0	0	0	0		0	0	12	Опрос
Тема2.	Система субъектов обеспечения информационной безопасности и их правовой статус.	20	4	0	0	4	0	0	0	0		0	0	12	Опрос
Тема3.	Преступность в	24	6	0	0	6	0	0	0	0		0	0		Опрос

	информационной сфере. Правовая защита личности. Способы защиты информации.												12	
Тема4.	Правовой режим и защита государственной или иной охраняемой законом тайны.	20	4	0	0	4	0	0	0	0	0	0	12	Опрос
Тема5.	Юридическая ответственность и предупреждение противоправных деяний в информационной сфере.	20	4	0	0	4	0	0	0	0	0	0	12	Опрос
Промежуточнаяаттестация		0	0	0	0	0	0	0	0	0	0	0	0	Зачет
Итого		108	24	0	0	24	0	0	0	0	0	0	60	

Заочная форма обучения

№ п/п	**Наименование тем и (или) разделов**		**Объемдисциплины, ак.час**		**Форма текущего контроля**
		ВСЕГО	**Контактная работа обучающихся с преподавателем по видам учебных занятий**	**Самостоятельнаяработа**	

			Периодтеоретическогообучения						Периодпромежуточнойаттестации (сессия)						успеваемости, промежуточной аттестации
			Занятиялекционноготипа		Занятиясеминарскоготипа		ИК	КСР	КЭ	Кат тэк	Контроль	СРкр	СРэк	СР	
			Л	ВЛ	ЛР	ПЗ									
Тема 1.	Информационная безопасность РоссийскойФедерации и задачи по ее обеспечению	14	2	0	0	0	0	0	0	0		0	0	12	Опрос
Тема2.	Система субъектов обеспечения информационной безопасности и их правовой статус.	14	2	0	0	0	0	0	0	0		0	0	12	Опрос
Тема3.	Преступность в информационной сфере. Правовая защита личности. Способы защиты	14	0	0	0	2	0	0	0	0		0	0	12	Опрос

	информации.													
Тема4.	Правовой режим и защита государственной или иной охраняемой законом тайны.	14	0	0	0	2	0	0	0	0	0	0	12	Опрос
Тема5.	Юридическая ответственность и предупреждение противоправных деяний в информационной сфере.	12	0	0	0	2	0	0	0	0	0	0	10	Опрос
Промежуточнаяаттестация		4	0	0	0	0	0	0	0	4	0	0	0	Зачет
Итого		108	6	0	0	8	0	0	0	4	0	0	90	

3.2. Содержание дисциплины

Тема 1.Информационная безопасность Российской Федерации и задачи по ее обеспечению.ПКр ОС-1.1.

Понятие информационной безопасности и информационного общества. Цели, задачи и принципы обеспечения информационной безопасности. Угроза национальной безопасности и их виды. Государственная политика Российской Федерации в сфере обеспечения информационной безопасности и ее принципы. Понятие правового обеспечения и правовой защиты. История формирования законодательства Российской Федерации об информации и ее защите. Система нормативно-правовых актов России, регулирующих отношения в сфере информационной безопасности. Международно-правовые нормы и стандарты в сфере информационной безопасности. Информационное право. Информационные отношения. Виды ведомственных и корпоративных норм и их место в системе правового регулирования информационной безопасности в Российской Федерации. Основные тенденции развития законодательства Российской Федерации в сфере информационной безопасности. Особенности стандартизации нормативной базы в сфере информационной безопасности в современном мире. Информация, ее виды и признаки. Информация как объект юридической защиты. Виды и источники информации, подлежащие защите.

Тема 2. Система субъектов обеспечения информационной безопасности и их правовой статус. ПКр ОС-1.1.

Понятие государственного управления в сфере обеспечения информационной безопасности. Система органов государственной власти, обеспечивающая информационной безопасности и особенности их компетентности. Правовой статус и система органов государственной власти, обеспечивающая право доступа к информации. Особенности правового статуса и организация работы органов государственной власти, обеспечивающих защиту информации, обрабатываемой техническими средствами.

Тема 3. Преступность в информационной сфере. Правовая защита личности. Способы защиты информации.ПКр ОС-1.1.

Понятие и виды преступности в информационной сфере. Основные этапы и тенденции развития компьютерной преступности в России. Особенности детерминации преступлений, совершаемых в информационной сфере. Криминологическая и криминалистическая характеристики основных способов мошенничества, совершаемых с помощью сети Интернет. Криминологическая и уголовно-правовая характеристика лиц, совершающих преступления в сфере компьютерной

информации. Система и структура нормативных актов, обеспечивающих защиту прав личности в информационной сфере. Конституционные гарантии правовой охраны прав личности в информационной сфере. Правовые средства защиты права на доступ к информации и неприкосновенности частной жизни. Правовой механизм защиты права на неприкосновенность частной жизни. Врачебная тайна как институт защиты интересов личности. Защита права на личную информацию с ограниченным доступом. Персональная тайна и ее виды. Обработка и правовая охрана персональных данных. Правовая база обеспечения защиты личности от воздействия «вредной» информации. Российская и зарубежная модели обеспечения защиты личности от воздействия «вредной» информации. Правовое обеспечение защиты информации, обрабатываемой вычислительной техникой и передаваемой по компьютерным цепям. Организационно-управленческие меры обеспечения защиты информации в сфере высоких технологий. Правовые основы применения «электронной цифровой подписи». Криптографическая защита информации. Контроль за разработкой, производством и применением криптографических средств, их правовая основа. Органы лицензирования и сертификации и их правовой статус.

Тема 4. Правовой режим и защита государственной или иной охраняемой законом тайны. ПКр ОС-1.1.

Понятие государственной тайны и правового режима ее обеспечения. Принципы и механизм отнесения сведений к государственной тайне. Процедура засекречивания и рассекречивания сведений, составляющих государственную тайну. Субъекты обеспечения режима государственной тайны и их правовой статус. Организационно-правовые меры защиты государственной тайны. Система контроля за режимом обеспечения государственной тайны.Понятие коммерческой тайны и ее правовой статус. Защита коммерческой тайны и патентование как способы правового закрепления права собственности на промышленный образец и полезную модель. Объекты защиты коммерческой тайны. Особенности правового обеспечения режима коммерческой тайны. Режим представления информации, составляющей коммерческую тайну органам государственной власти.

Тема 5. Юридическая ответственность и предупреждение противоправных деяний в информационной сфере.ПКр ОС-1.1.

Информационная безопасность России и задачи по ее обеспечению. Субъекты деятельности по обеспечению противодействия правонарушениям в сфере информационной безопасности и их правовой статус. Оперативно-розыскные и криминалистические мероприятия по борьбе с преступлениями в сфере информационной безопасности. Особенности расследования преступлений в сфере информационной

безопасности. Совершенствование правовых норм как средство обеспечения профилактического воздействия на отношения в сфере ИБ. Зарубежный опыт борьбы с преступностью в сфере информационной безопасности. Понятие и виды юридической ответственности за правонарушения в сфере информационной безопасности. Уголовная ответственность за правонарушения в сфере информационной безопасности и ее особенности. Объективные и субъективные признаки составов преступлений, посягающих на информационной безопасности страны. Составы административных правонарушений, посягающих на информационной безопасности страны. Органы государственной власти и должностные лица, уполномоченные рассматривать административные правонарушения в сфере защиты информации и их правовой статус.

4. Типы оценочных материалов, показатели и критериоценивания

4.1. Оценочные материалы по дисциплине Б1.В.02.05Правовое обеспечение информационной безопасностивходят в состав оценочных материалов по образовательной программе. Совокупность оценочных материалов по всем дисциплинам (модулям) образовательной программы составляют фонд оценочных средств (далее – ФОС). ФОС используется при проведении текущего контроля успеваемости и промежуточной аттестации обучающихся с целью оценивания достижения обучающимися планируемых результатов обучения.

4.2. ФОС разработан как комплекс проверочных заданий различного типа и уровня сложности, включает критерии и шкалы оценивания, а также «ключи» правильных ответов. ФОС формируется как отдельный документ и хранится в электронном виде, доступ к ФОС предоставлен ограниченному кругу лиц.

4.3. Для самостоятельной работы обучающихся при подготовке к текущему контролю успеваемости и промежуточной аттестации в рабочих программах дисциплин размещены типовые проверочные задания, которые можно условно разделить на задания закрытого, комбинированного и открытого типов.

Задания закрытого типа – это тестовые задания, в которых каждый вопрос сопровождается готовыми вариантами ответов, из которых необходимо выбрать один или несколько правильных.

Задания комбинированного типа – это тестовые задания, в которых каждый вопрос сопровождается готовыми вариантами ответов, из которых необходимо выбрать один или несколько правильных и обосновать свой выбор.

Задания открытого типа – это задания, в которых на каждый вопрос должен быть предложен развернутый обоснованный ответ.

В зависимости от типа задания рекомендованы определенная последовательность выполнения и система оценивания выполнения заданий.

4.4. Типы заданий, сценарии выполнения, критерии оценивания

ТИП ЗАДАНИЯ	ИНСТРУКЦИЯ	СЦЕНАРИИ ВЫПОЛНЕНИЯ	КРИТЕРИИ ОЦЕНИВАНИЯ
Задание закрытого типа с выбором одного правильного ответа из нескольких вариантов предложенных	Прочитайте текст, выберите правильный ответ	1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. 2. Внимательно прочитать предложенные варианты ответа. 3. Выбрать один верный ответ. 4. Записать только номер (или букву) выбранного варианта ответа (например, 3 или В).	Ответ считается верным, если правильно указана цифра или буква
Задание закрытого типа на установление соответствия	Прочитайте текст и установите соответствие	1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидаются пары элементов. 2. Внимательно прочитать оба списка: список 1 – вопросы, утверждения, факты, понятия и т.д.; список 2 – утверждения, свойства объектов и т.д. 3. Сопоставить элементы списка 1 с элементами списка 2, сформировать пары элементов. 4. Записать попарно буквы и цифры (в зависимости от задания) вариантов ответа (например, А1 или Б4).	Ответ считается верным, если правильно указаны цифры или буквы
Задание закрытого типа с выбором нескольких правильных ответов из нескольких вариантов предложенных	Прочитайте текст, выберите правильные ответы	1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидается несколько правильных ответов из предложенных вариантов. 2. Внимательно прочитать предложенные вариант-ты ответа. 3. Выбрать несколько правильных ответов. 4. Записать только номера (или буквы) выбранного варианта ответа (например, 1 4 или А Г).	Ответ считается верным, если правильно установлены все соответствия (позиции из одного столбца верно сопоставлены с позициями другого)
Задание закрытого типа на установление	Прочитайте текст и установите	1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается	Ответ считается верным, если правильно указана вся

последовательности	последовательность	последовательность элементов. 2. Внимательно прочитать предложенные варианты ответа. 3. Построить верную последовательность из предложенных элементов. 4. Записать буквы/цифры (в зависимости от задания) вариантов ответа в нужной последовательности (например, БВА или 135).	последовательность цифр
Задание комбинированного типа с выбором одного правильного ответа из предложенных и обоснованием выбора	Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа	1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. 2. Внимательно прочитать предложенные варианты ответа. 3. Выбрать один верный ответ. 4. Записать только номер (или букву) выбранного варианта ответа. 5. Записать аргументы, обосновывающие выбор ответа (например, 4 текст обоснования).	Ответ считается верным, если правильно указана цифра или буква и приведены корректные аргументы, используемые при выборе ответа
Задание открытого типа с развернутым ответом	Прочитайте текст и запишите развернутый обоснованный ответ	1. Внимательно прочитать текст задания и понять суть вопроса. 2.Продумать логику и полноту ответа. 3.Записать ответ, используя четкие компактные формулировки. 4.В случае расчетной задачи, записать решение и ответ	Ответ считается верным: 1. Отсутствие фактических ошибок. 2. Раскрытие объема используемых понятий (полнота ответа). 3.Обоснованность ответа (наличие аргументов). 4. Логическая последовательность излагаемого материала.

4.5. Общая шкала оценивания результатов текущего контроля успеваемости и промежуточной аттестации обучающихся

Традиционная система	Бинарная система	ECTS	
		Для традиционной системы	Для бинарной системы
Отлично	Зачтено	A	P/ Passed
		B	P/ Passed
Хорошо		C	P/ Passed
		D	P/ Passed
Удовлетворительно		E	P/ Passed
Неудовлетворительно	Не зачтено	F	F/Failed

5. Формы аттестации, типовые оценочные материалы для текущего контроля успеваемости обучающихся, критерии и шкалы оценивания

5.1. В ходе реализации дисциплины Б1.В.02.05Правовое обеспечение информационной безопасностииспользуются следующие формы текущего контроля успеваемости обучающихся:

опрос.

5.2. Типовые оценочные материалы для текущего контроля успеваемости обучающихся:

Тема 1.Информационная безопасность Российской Федерации и задачи по ее обеспечению.ПКр ОС-1.1.

Вопросы для опроса:

1. Понятие информационной безопасности и информационного общества.
2. Цели, задачи и принципы обеспечения информационной безопасности.
3. Угроза национальной безопасности и их виды.
4. Государственная политика Российской Федерации в сфере обеспечения информационной безопасности и ее принципы.
5. Понятие правового обеспечения и правовой защиты.
6. История формирования законодательства Российской Федерации об информации и ее защите.
7. Система нормативно-правовых актов России, регулирующих отношения в сфере информационной безопасности.

8. Международно-правовые нормы и стандарты в сфере информационной безопасности.

9. Информация, ее виды и признаки. Информация как объект юридической защиты.

10. Виды и источники информации, подлежащие защите.

Тема 2. Система субъектов обеспечения информационной безопасности и их правовой статус. ПКр ОС-1.1.

Вопросы для опроса:

1. Понятие государственного управления в сфере обеспечения информационной безопасности.

2. Система органов государственной власти, обеспечивающая информационной безопасности и особенности их компетентности.

3. Правовой статус и система органов государственной власти, обеспечивающая право доступа к информации.

4. Особенности правового статуса и организация работы органов государственной власти, обеспечивающих защиту информации, обрабатываемой техническими средствами.

Тема 3. Преступность в информационной сфере. Правовая защита личности. Способы защиты информации. ПКр ОС-1.1.

Вопросы для опроса:

1. Понятие и виды преступности в информационной сфере.

2. Криминологическая и криминалистическая характеристики основных способов мошенничества, совершаемых с помощью сети Интернет.

3. Криминологическая и уголовно-правовая характеристика лиц, совершающих преступления в сфере компьютерной информации.

4. Система и структура нормативных актов, обеспечивающих защиту прав личности в информационной сфере.

5. Правовые средства защиты права на доступ к информации и неприкосновенности частной жизни. Правовой механизм защиты права на неприкосновенность частной жизни.

6. Обработка и правовая охрана персональных данных.

7. Организационно-управленческие меры обеспечения защиты информации в сфере высоких технологий.

8. Правовые основы применения «электронной цифровой подписи». Криптографическая защита информации.

9. Контроль за разработкой, производством и применением криптографических средств, их правовая основа.

10. Органы лицензирования и сертификации и их правовой статус.

Тема 4. Правовой режим и защита государственной или иной охраняемой законом тайны. ПКр ОС-1.1.

Вопросы для опроса:

1. Понятие государственной тайны и правового режима ее обеспечения.
2. Принципы и механизм отнесения сведений к государственной тайне.
3. Процедура засекречивания и рассекречивания сведений, составляющих государственную тайну.
4. Субъекты обеспечения режима государственной тайны и их правовой статус.
5. Организационно-правовые меры защиты государственной тайны. Система контроля за режимом обеспечения государственной тайны.
6. Понятие коммерческой тайны и ее правовой статус.
7. Защита коммерческой тайны и патентование как способы правового закрепления права собственности на промышленный образец и полезную модель.
8. Объекты защиты коммерческой тайны.
9. Режим представления информации, составляющей коммерческую тайну органам государственной власти.

Тема 5. Юридическая ответственность и предупреждение противоправных деяний в информационной сфере.ПКр ОС-1.1.

Вопросы для опроса:

1. Информационная безопасность России и задачи по ее обеспечению.
2. Субъекты деятельности по обеспечению противодействия правонарушениям в сфере информационной безопасности и их правовой статус.
3. Особенности расследования преступлений в сфере информационной безопасности.
4. Зарубежный опыт борьбы с преступностью в сфере информационной безопасности.
5. Понятие и виды юридической ответственности за правонарушения в сфере информационной безопасности.
6. Уголовная ответственность за правонарушения в сфере информационной безопасности и ее особенности.
7. Составы административных правонарушений, посягающих на информационной безопасности страны.

6. Формы промежуточной аттестации, критерии и шкала оценивания, типовые оценочные материалы по дисциплине

6.1. Промежуточная аттестация (зачет)проводится в устной форме.

Обучающийся получает экзаменационный билет с вариантами

вопросов. Обучающийся приступает к подготовке к ответу. Время на подготовку – 30 минут.Обучающийся отвечает на каждый вопрос в билете, демонстрируя свои знания и умения. При необходимости обучающийся отвечает на дополнительные вопросы преподавателя.

6.2. Типовые оценочные материалы промежуточной аттестации

Типовые проверочные задания для самоподготовки обучающегося к промежуточной аттестации:

Тема 1.Информационная безопасность Российской Федерации и задачи по ее обеспечению.ПКр ОС-1.1.

1. Задания открытого типа.
1.1. Вопросы открытого типа.

№ п.п.	Вопрос
1.	Информационная безопасность: понятие, основные задачи и методы ее обеспечения.
2.	Угрозы информационной безопасности.
3.	Государственная политика в сфере информационной безопасности.
4.	Основные задачи по обеспечению информационной безопасности.
5.	Система нормативно-правовых актов России, регулирующих отношения в сфере информационной безопасности.
6.	8. Международно-правовые нормы и стандарты в сфере информационной безопасности.
7.	9. Информация, ее виды и признаки. Информация как объект юридической защиты.
8.	10. Виды и источники информации, подлежащие защите.

Тема 2. Система субъектов обеспечения информационной безопасности и их правовой статус. ПКр ОС-1.1.

1. Задания открытого типа.
1.1. Вопросы открытого типа.

№ п.п.	Вопрос
1.	Субъект информационной безопасности: понятие, виды.
2.	Государственное управление в информационной сфере.
3.	Правовой статус и система органов государственной власти, обеспечивающая право доступа к информации.
4.	4. Особенности правового статуса и организация работы органов государственной власти, обеспечивающих защиту информации, обрабатываемой техническими средствами.

Тема 3. Преступность в информационной сфере. Правовая защита личности. Способы защиты информации. ПКр ОС-1.1.

1. Задания открытого типа.
1.1. Вопросы открытого типа.

№ п.п.	Вопрос
1.	Понятие и виды преступности в информационной сфере.
2.	Криминологическая и уголовно-правовая характеристика лиц, совершающих преступления в сфере компьютерной информации.
3.	Система и структура нормативных актов, обеспечивающих защиту прав личности в информационной сфере.
4.	Правовые средства защиты права на доступ к информации и неприкосновенности частной жизни.
5.	Органы лицензирования и сертификации и их правовой статус.

Тема 4. Правовой режим и защита государственной или иной охраняемой законом тайны. ПКр ОС-1.1.

1. Задания открытого типа.
1.1. Вопросы открытого типа.

№ п.п.	Вопрос
1.	Понятие государственной тайны и правового режима ее обеспечения.
2.	Принципы и механизм отнесения сведений к государственной тайне.
3.	Процедура засекречивания и рассекречивания сведений, составляющих государственную тайну.
4.	Субъекты обеспечения режима государственной тайны и их правовой статус.
5.	Организационно-правовые меры защиты государственной тайны.
6.	Понятие коммерческой тайны и ее правовой статус.
7.	Защита коммерческой тайны и патентование как способы правового закрепления права собственности на промышленный образец и полезную модель.
8.	Объекты защиты коммерческой тайны.

Тема 5. Юридическая ответственность и предупреждение противоправных деяний в информационной сфере.ПКр ОС-1.1.

1. Задания открытого типа.
1.1. Вопросы открытого типа.

№	Вопрос

п.п.	
1.	Меры предупреждения преступности в информационной сфере в современной России
2.	Понятие и виды преступлений в информационной сфере.
3.	Уголовно-правовая характеристика преступлений в информационной сфере.
4.	Особенности расследования преступлений в сфере информационной безопасности.
5.	Составы административных правонарушений, посягающих на информационной безопасности страны.

6.3. Критерии и шкала оценивания.

КРИТЕРИИ ОЦЕНИВАНИЯ	РЕЗУЛЬТАТ
Дан ответ на поставленный вопрос, где обучающийся демонстрирует знания, приобретенные на лекционных и семинарских занятиях, а также полученные посредством изучения обязательных учебных материалов по курсу, дает ответы, приводит примеры, в ответе присутствует владение монологической речью, логичность и последовательность ответа. Допускаютсянеточности в ответе.	зачтено
Дан ответ, который содержит ряд серьезных неточностей, обнаруживающий незнание процессов изучаемой предметной области, отличающийся неглубоким раскрытием темы, незнанием основных вопросов теории, несформированными навыками анализа явлений, процессов, неумением давать аргументированные ответы, слабым владением монологической речью, отсутствием логичности и последовательности. Выводы поверхностны. Решение практических заданий не выполнено, т.е. обучающийся не способен ответить на вопросы даже при дополнительных наводящих вопросах преподавателя.	Незачтено

7. Методические материалы по освоению дисциплины (модуля)

Подготовка к лекциям.

Главное в период подготовки к лекционным занятиям – научиться методам самостоятельного умственного труда, сознательно развивать свои творческие способности и овладевать навыками творческой работы. Для этого необходимо строго соблюдать дисциплину учебы и поведения. Четкое планирование своего рабочего времени и отдыха является необходимым условием для успешной самостоятельной работы. В основу его нужно положить рабочие программы изучаемых в семестре дисциплин.Каждому

обучающемуся следует составлять еженедельный и семестровый планы работы, а также план на каждый рабочий день. С вечера всегда надо распределять работу на завтрашний день. В конце каждого дня целесообразно подводить итог работы: тщательно проверить, все ли выполнено по намеченному плану, не было ли каких-либо отступлений, а если были, по какой причине это произошло. Нужно осуществлять самоконтроль, который является необходимым условием успешной учебы. Если что-то осталось невыполненным, необходимо изыскать время для завершения этой части работы, не уменьшая объема недельного плана.

Самостоятельная работа на лекции.

Слушание и запись лекций – сложный вид вузовской аудиторной работы. Внимательное слушание и конспектирование лекций предполагает интенсивную умственную деятельность обучающегося. Краткие записи лекций, их конспектирование помогает усвоить учебный материал. Конспект является полезным тогда, когда записано самое существенное, основное и сделано это самим обучающимся. Не надо стремиться записать дословно всю лекцию. Такое «конспектирование» приносит больше вреда, чем пользы. Запись лекций рекомендуется вести по возможности собственными формулировками. Желательно запись осуществлять на одной странице, а следующую оставлять для проработки учебного материала самостоятельно в домашних условиях. Конспект лекции лучше подразделять на пункты, параграфы, соблюдая красную строку. Этому в большой степени будут способствовать пункты плана лекции, предложенные преподавателям. Принципиальные места, определения, формулы и другое следует сопровождать замечаниями «важно», «особо важно», «хорошо запомнить» и т.п. Можно делать это и с помощью разноцветных маркеров или ручек. Лучше если они будут собственными, чтобы не приходилось просить их у однокурсников и тем самым не отвлекать их во время лекции. Целесообразно разработать собственную «маркографию» (значки, символы), сокращения слов. Не лишним будет и изучение основ стенографии. Работая над конспектом лекций, всегда необходимо использовать не только учебник, но и ту литературу, которую дополнительно рекомендовал лектор. Именно такая серьезная, кропотливая работа с лекционным материалом позволит глубоко овладеть знаниями.

Подготовка к практическим занятиям.

Подготовку к каждому практическому занятию каждый обучающийся должен начать с ознакомления с планом практического занятия, который отражает содержание предложенной темы. Тщательное продумывание и изучение вопросов плана основывается на проработке текущего материала лекции, а затем изучения обязательной и дополнительной литературы, рекомендованную к данной теме. На основе индивидуальных предпочтений обучающемуся необходимо самостоятельно выбрать тему доклада по проблеме практического занятия и по возможности подготовить по нему презентацию.

Если программой дисциплины предусмотрено выполнение практического задания, то его необходимо выполнить с учетом предложенной инструкции (устно или 10 письменно). Все новые понятия по изучаемой теме необходимо выучить наизусть и внести в глоссарий, который целесообразно вести с самого начала изучения курса. Результат такой работы должен проявиться в способности обучающегося свободно ответить на теоретические вопросы практического занятия, его выступлении и участии в коллективном обсуждении вопросов изучаемой темы, правильном выполнении практических заданий и контрольных работ.

Структура практического занятия:

В зависимости от содержания и количества отведенного времени на изучение каждой темы может практическое занятие состоять из четырех-пяти частей:

1. Обсуждение теоретических вопросов, определенных программой дисциплины.
2. Доклад и/ или выступление с презентациями по проблеме практического занятия.
3. Обсуждение выступлений по теме – дискуссия.
4. Выполнение практического задания с последующим разбором полученных результатов или обсуждение практического задания, выполненного дома, если это предусмотрено программой.
5. Подведение итогов занятия.

Первая часть – обсуждение теоретических вопросов - проводится в виде фронтальной беседы со всей группой и включает выборочную проверку преподавателем теоретических знаний обучающихся. Примерная продолжительность — до 15 минут. Вторая часть — выступление обучающихся с докладами, которые должны сопровождаться презентациями с целью усиления наглядности восприятия, по одному из вопросов практического занятия. Обязательный элемент доклада – представление и анализ статистических данных, обоснование социальных последствий любого экономического факта, явления или процесса. Примерная продолжительность — 20-25 минут. После докладов следует их обсуждение – дискуссия. В ходе этого этапа практического занятия могут быть заданы уточняющие вопросы к докладчикам. Примерная продолжительность – до 15-20 минут. Если программой предусмотрено выполнение практического задания в рамках конкретной темы, то преподавателями определяется его содержание и дается время на его выполнение, а затем идет обсуждение результатов. Если практическое задание должно было быть выполнено дома, то на практическом занятии преподаватель проверяет его выполнение (устно или письменно). Примерная продолжительность – 15-20 минут. Подведением итогов заканчивается практическое занятие. Обучающимся должны быть объявлены оценки за работу и даны их четкие обоснования. Примерная продолжительность — 5 минут.

Работа с литературными источниками.

В процессе подготовки к практическим занятиям, обучающимся необходимо обратить особое внимание на самостоятельное изучение рекомендованной учебно-методической (а также научной и популярной) литературы. Самостоятельная работа с учебниками, учебными пособиями, научной, справочной и популярной литературой, материалами периодических изданий и Интернета, статистическими данными является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у обучающихся свое отношение к конкретной проблеме. Более глубокому раскрытию вопросов способствует знакомство с дополнительной литературой, рекомендованной преподавателем, что позволяет обучающимся проявить свою индивидуальность в рамках выступления на занятиях, выявить широкий спектр мнений по изучаемой проблеме.

Самостоятельная работа студентов.

Это основной вид деятельности студента, включающий в себя изучение лекционного материала, учебников и учебных пособий, первоисточников, подготовку сообщений, выступления на групповых занятиях, выполнение заданий преподавателя.

Методика самостоятельной работы предварительно разъясняется преподавателем и в последующем может уточняться с учетом индивидуальных особенностей студентов. Время и место самостоятельной работы выбираются студентами по своему усмотрению с учетом рекомендаций преподавателя.

Самостоятельную работу над дисциплиной следует начинать с изучения программы, которая содержит основные требования к знаниям, умениям и навыкам обучаемых. Обязательно следует вспомнить рекомендации преподавателя, данные в ходе установочных занятий. Затем – приступать к изучению отдельных разделов и тем в порядке, предусмотренном программой.

Получив представление об основном содержании раздела, темы, необходимо изучить материал с помощью учебника. Целесообразно составить краткий конспект или схему, отображающую смысл и связи основных понятий данного раздела и включенных в него тем. Затем, как показывает опыт, полезно изучить выдержки из первоисточников. При желании можно составить их краткий конспект. Обязательно следует записывать возникшие вопросы, на которые не удалось ответить самостоятельно.

Подготовка к зачету.

К зачету необходимо готовится целенаправленно, регулярно, систематически и с первых дней обучения по данной дисциплине. Попытки освоить дисциплину в период зачётно-экзаменационной сессии, как правило, показывают не слишком удовлетворительные результаты. В самом начале учебного курса познакомьтесь со следующей учебно-методической документацией:

- программой дисциплины;
- перечнем знаний и умений, которыми студент должен владеть;
- тематическими планами лекций, практических и лабораторных занятий;
- контрольными мероприятиями;
- учебником, учебными пособиями по дисциплине, а также электронными ресурсами;
- перечнем вопросов для зачета.

После этого у вас должно сформироваться четкое представление об объеме и характере знаний, которыми надо будет овладеть по дисциплине. Систематическое выполнение учебной работы на лекциях, практических и лабораторных занятиях позволит успешно освоить дисциплину и создать хорошую базу для сдачи зачета.

8. Учебная литература и ресурсы информационно-телекоммуникационной сети Интернет

8.1. Основная литература

1. Организационно-техническое и правовое обеспечение информационной безопасности Российской Федерации : учебник / сост. И. Г. Дровникова, А. В. Калач, И. И. Лившиц [и др]. - Воронеж : Научная книга, 2022. - 304 с. - ISBN 978-5-4446-1743-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/1999941 (дата обращения: 19.07.2026). – Режим доступа: по подписке.

2. Организационно-правовое обеспечение информационной безопасности : учебник / под ред. А. А. Александрова, М. П. Сычева. - Москва : МГТУ им. Баумана, 2018. - 292 с. - ISBN 978-5-7038-4723-7. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2010603 (дата обращения: 19.07.2026). – Режим доступа: по подписке.

8.2. Дополнительная литература

1. Куняев, Н. Н. Правовое обеспечение национальных интересов Российской Федерации в информационной сфере : монография / Н. Н. Куняев. — Москва : Логос, 2020. — 348 с. — ISBN 978-5-98704-513-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL:

https://e.lanbook.com/book/163040 (дата обращения: 19.07.2026). — Режим доступа: для авториз. пользователей.

2. Мальцев, В. А. Правовое обеспечение информационной безопасности в российской федерации : учебно-методическое пособие / В. А. Мальцев. — Воронеж : ВГУ, 2017. — 40 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/154824 (дата обращения: 19.07.2026). — Режим доступа: для авториз. пользователей.

8.3. Нормативные правовые документы и иная правовая информация

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ, от 14.03.2020 № 1-ФКЗ; от 04.10.2022 № 8-ФКЗ// Российская газета. – 1993. – № 237; СЗ РФ. – 2022. – № 41. – Ст. 6933.

2. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (с изменениями и дополнениями) // Российская газета, № 249, 22.12.2001.

3. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (с изменениями и дополнениями) // СЗ РФ. 1996. № 25. Ст. 2954

4. Закон РФ «О государственной тайне» от 21 июля 1993 г. (с изменениями и дополнения-ми) // СЗ РФ, 1997. № 41. Ст. 4673.

5. Федеральный закон «Об оперативно-розыскной деятельности» от 12 августа 1995 г. № 144-ФЗ (с изменениями и дополнениями) // СЗ РФ. 1995. № 33. Ст. 3349.

6. Указ Президента РФ от 24 января 1998 г. «О Перечне сведений, отнесенных к государственной тайне» (с изменениями и дополнениями) // РГ. 1998. 3 февраля.

8.4. Интернет-ресурсы

1. www.ks.rfnet.ru – Официальный сайт Конституционного Суда Российской Федерации.
2. www.vsrf.ru – Официальный сайт Верховного Суда Российской Федерации.
3. www.ombudsmanrf.ru – Официальный сайт Уполномоченного по правам человека России.
4. www.inion.ru – Институт научной информации по общественным наукам РАН.
5. www.igpan.ru/rus/magazine.ru – Журнал «Государство и право».
6. www.iprbookshop.ru – IPRbooks электронно-библиотечная система.

7. www.e.lanbook.com – Издательство «Лань». Электронно-библиотечная система.
8. www.biblio-online.ru – Электронно-библиотечная система ЮРАЙТ.
9. www.rsl.ru – Российская Государственная Библиотека.
10. www.nnir.ru – Российская национальная библиотека.
11. www.nns.ru – Национальная электронная библиотека.
12. www.rsi.ru – Российская государственная библиотека.
13. www.elibrary.ru – Электронная библиотека журналов.
14. www.consultant.ru – справочная система КонсультантПлюс.
15. www.garant.ru – справочная система Гарант.
16. www.yandex.ru – Поисковая система.
17. www.orel.ranepa.ru – Официальный портал СИУ РАНХиГС.

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

Требования к аудитории:
- Лекционные
- Семинарские
- Помещения для самостоятельной работы

Требования к оборудованию:
- Учебная мебель
- Доска
- проектор
-Компьютер (стационарный) или ноутбук

Требования к программному обеспечению:

Наименование программного обеспечения	**Назначение**
7-Zip	Архиватор с высокой степенью сжатия Свободная лицензия
Adobe Acrobat	Чтение, печать и рецензирование файлов PDF. Свободная лицензия
Adobe reader	Просмотр, печать и внесение аннотаций в документы PDF. Свободная лицензия
Kaspersky Endpoint Security	Антивирусное ПО
MS Office	Пакет офисных приложений.
MS Visual Studio	интегрированная среда разработки (IDE), созданная

2022	компанией Microsoft. Предназначена для разработки программного обеспечения на различных языках программирования, включая C#, VB.NET, C++, Python и другие
Mts-linkTelemost	Экосистема сервисов для бизнес-коммуникаций и совместной работы.
MySQL	система управления реляционными базами данных (СУБД)
MySQL Workbench	Инструмент для визуального проектирования баз данных, интегрирующий проектирование, моделирование, создание и эксплуатацию БД в единое бесшовное окружение для системы баз данных MySQL. Версия CommunityEdition — распространяетсяпосвободнойлицензиейGNUGPL.
Open Office	Свободный пакет офисных приложений. Свободная лицензия
Yandex Browser	Браузер Свободная лицензия
Yandex Messenger	приложение для общения, групповых чатов, а также аудио – и видеозвонков
ГАРАНТ	Справочно-правовая система
Консультант Плюс	Справочно-правовая система
Яндекс Диск	облачное хранилище для файлов, данных и видео от Яндекс
Яндекс Календарь	бесплатный персональный информационный менеджер
Яндекс Телемост	это сервис для видеовстреч без ограничений по времени