

Федеральное государственное бюджетное образовательное учреждение высшего образования «Тамбовский государственный университет имени Г.Р. Державина»
Институт права и национальной безопасности
Кафедра специальной подготовки и обеспечения национальной безопасности

УТВЕРЖДАЮ:
Директор института



В. А. Шуняева
«21» января 2021 г.

РАБОЧАЯ ПРОГРАММА

по дисциплине Б1.В.ОД.12 Правовое регулирование информационной безопасности

Направление подготовки/специальность: 40.05.01 - Правовое обеспечение национальной безопасности

Профиль/направленность/специализация: Уголовно-правовая

Уровень высшего образования: специалитет

Квалификация: Юрист

год набора: 2019

Тамбов, 2021

Автор программы:

Кандидат технических наук, доцент Терехов Алексей Васильевич

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 40.05.01 - Правовое обеспечение национальной безопасности (уровень специалитета) (приказ Министерства образования и науки РФ от «19» декабря 2016 г. № 1614).

Рабочая программа принята на заседании Кафедры специальной подготовки и обеспечения национальной безопасности «20» января 2021 г. Протокол № 7

Рассмотрена и одобрена на заседании Ученого совета Института права и национальной безопасности, Протокол от «21» января 2021 г. № 5.

СОДЕРЖАНИЕ

1. Цели и задачи дисциплины.....	4
2. Место дисциплины в структуре ОП Специалиста.....	7
3. Объем и содержание дисциплины.....	7
4. Контроль знаний обучающихся и типовые оценочные средства.....	13
5. Методические указания для обучающихся по освоению дисциплины (модуля).....	27
6. Учебно-методическое и информационное обеспечение дисциплины.....	29
7. Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы.....	29

1. Цели и задачи дисциплины

1.1 Цель дисциплины – формирование компетенций:

ОК-12 Способность работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации

ПК-6 Способность квалифицированно толковать нормативные правовые акты

ПК-16 Способность соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности

1.2 Виды и задачи профессиональной деятельности по дисциплине:

- правоохранительная
- экспертно-консультационная

1.3 В результате освоения дисциплины у обучающихся должны быть сформированы следующие компетенции:

Обобщенные трудовые функции / трудовые функции / трудовые или профессиональные действия (при наличии профстандарта)	Код и наименование компетенции ФГОС ВО, необходимой для формирования трудового или профессионального действия	Знания и умения, необходимые для формирования трудового действия / компетенции
	ОК-12 Способность работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации	Знает и понимает: основные понятия и концепции современных технологий защиты информации; основные методы создания систем защиты информации; основные стандарты в области информационной безопасности; основные инструментальные средства защиты информации; источники возникновения информационных угроз; модели и принципы защиты информации от несанкционированного доступа; методы антивирусной защиты информации; состав и методы организационно-правовой защиты информации.
		Умеет (способен продемонстрировать): Умеет (способен продемонстрировать): анализировать типы атак и угроз информационной безопасности; формулировать соответствующие требования к системам защиты информации; применять правовые, организационные, технические и программные средства защиты информации.
		Владеет: Владеет базовыми навыками построения и управления систем защиты информации; навыками отражения типовых атак на информационные системы; базовыми навыками безопасной работы в компьютерных сетях при сборе, передаче и преобразовании информации; методами антивирусной защиты технических средств обработки информации..
	ПК-6 Способность	Знает и понимает:

	<p>квалифицированно толковать нормативные правовые акты</p>	<p>Знает и понимает: юридические понятия и конструкции; основные понятия и определения информационной безопасности, модели информационной безопасности, политику безопасности компании в области информационной безопасности; основы криптографических методов защиты информации; принципы проектирования защищенных баз данных; способы защиты программного обеспечения от несанкционированного распространения и модификации</p> <p>Умеет (способен продемонстрировать):</p> <p>Умеет (способен продемонстрировать): анализировать источники, риски и формы атак на информацию, толковать и правильно понимать угрозы, которыми подвергается информация, понимает политики безопасности и умеет управлять полномочиями и протоколами идентификации и аутентификации пользователей в СУБД и ОС; использовать методы и средства обеспечения информационной безопасности с целью предотвращения несанкционированного доступа, злоумышленной модификации или утраты информации, составляющей государственную тайну и иной служебной информации;</p> <p>Владеет:</p> <p>работы с нормативными правовыми актами; навыками использования и конфигурирования штатных средств обеспечения информационной безопасности ИС, и распространенных программных средств;</p>
	<p>ПК-16 Способность соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности</p>	<p>Знает и понимает:</p> <p>Знает и понимает: основные понятия и определения, используемые при изучении информационной безопасности; классификацию угроз информационной безопасности; классические и современные методы взлома сетевых носителей и систем; классификацию компьютерных вирусов, какую угрозу они представляют для безопасности информации и правила защиты от компьютерных вирусов и вредоносных программ; как организовать информационную безопасность в организации; нормы и требования российского законодательства в области защиты информации.</p> <p>Умеет (способен продемонстрировать):</p> <p>Умеет (способен продемонстрировать): правильно выбирать и использовать антивирусную защиту; восстанавливать пораженные компьютерными вирусами объекты средствами выбранной антивирусной защиты; осуществлять профессиональную деятельность с использованием информационно-правовых систем и иного программного обеспечения в сети Internet с соблюдением требований информационной безопасности.</p> <p>Владеет:</p>

		Владеет навыками: навыками подбора и применения современных методов и способов защиты информации; работы с нормативными документами России в области защиты информации и обеспечения ее конфиденциальности; обеспечения соблюдения требований законодательства РФ о защите персональных данных.
--	--	---

1.4 Согласование междисциплинарных связей дисциплин, обеспечивающих освоение компетенций:

ОК-12 Способность работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации

№ п/п	Наименование дисциплин, определяющих междисциплинарные связи	Форма обучения					
		Очная (семестр)			Заочная (семестр)		
		1	2	5	1	2	5
1	Введение в проектную деятельность		+			+	
2	Информатика и информационные технологии в профессиональной деятельности	+			+		
3	Правовая защита персональных данных			+			+

ПК-6 Способность квалифицированно толковать нормативные правовые акты

№ п/п	Наименование дисциплин, определяющих междисциплинарные связи	Форма обучения																	
		Очная (семестр)									Заочная (семестр)								
		1	2	3	4	5	6	7	8	9	1	2	3	4	5	6	7	8	9
1	Административное право				+									+					
2	Гражданское право			+	+	+	+						+	+	+	+			
3	Гражданское процессуальное право (гражданский процесс)						+	+								+	+		
4	Конституционное право России			+									+						
5	Практика по получению профессиональных умений и опыта профессиональной деятельности								+									+	
6	Теория государства и права	+	+								+	+							

7	Уголовно-правовое и криминологическое обеспечение борьбы с незаконным оборотом наркотических средств							+									+		
8	Уголовное право			+	+	+	+						+	+	+	+			
9	Экологическое право								+										+

ПК-16 Способность соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности

№ п/п	Наименование дисциплин, определяющих междисциплинарные связи	Форма обучения									
		Очная (семестр)				Заочная (семестр)					
		2	4	5	10	2	4	5	10	11	
1	Актуальные вопросы обеспечения национальной безопасности				+				+		
2	Основы теории национальной безопасности		+	+			+	+			
3	Правовая защита персональных данных			+				+			
4	Правоохранительные органы	+				+					
5	Преддипломная практика				+					+	
6	Уголовно-правовая политика в области обеспечения национальной безопасности			+				+			

2. Место дисциплины в структуре ОП специалитета:

Дисциплина «Правовое регулирование информационной безопасности» относится к вариативной части учебного плана ОП по направлению подготовки 40.05.01 - Правовое обеспечение национальной безопасности.

Дисциплина «Правовое регулирование информационной безопасности» изучается в 3 семестре.

3. Объем и содержание дисциплины

3.1. Объем дисциплины: 4 з.е.

Очная: 4 з.е.

Заочная: 4 з.е.

Вид учебной работы	Очная (всего часов)	Заочная (всего часов)
Общая трудоёмкость дисциплины	144	144
Контактная работа	48	14
Лекции (Лекции)	16	6

Практические (Практ. раб.)	32	8
Самостоятельная работа (СР)	60	121
Экзамен	36	9

3.2.Содержание курса:

№ темы	Название раздела/темы	Вид учебной работы, час.						Формы текущего контроля
		Лекции		Практ. раб.		СР		
		О	З	О	З	О	З	
3 семестр								
1	Тема 1. Введение в ин-формационную безопас-ность	2	1	4	1	6	20	Опрос; Реферат
2	Тема 2. Правовое обеспечение информационной безопасности	2	1	4	2	8	21	Опрос; Реферат
3	Тема 3. Организационное обеспечение информационной безопасности. Механизмы обеспечения "информационной безопасности"	4	1	6	1	12	20	Опрос; Реферат; Тестирование
4	Тема 4. Программно-аппаратные средства и методы обеспечения ин-формационной безопас-ности	2	1	8	1	12	20	Опрос; Реферат
5	Тема 5. Криптографиче-ские методы защиты ин-формации	2	1	4	1	10	20	Опрос; Реферат
6	Тема 6. Компьютерные вирусы и методы антивирусной защиты. Информационная безопасность вычислительных сетей	4	1	6	2	12	20	Опрос; Реферат; Тестирование

Тема 1. Тема 1. Введение в ин-формационную безопас-ность

Лекция.

Информационная безопасность. Основные понятия. Модели информационной безопасности. Виды защищаемой информации. Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности. Международные стандарты информационного обмена. Классификация компьютерных преступлений. Способы совершения компьютерных преступлений. Пользователи и злоумышленники в Internet. Причины уязвимости сети Internet. Понятия и определения в информационной безопасности.

Практическое занятие.

1. Виды угроз информационной безопасности. Три вида возможных нарушений информационной системы. Защита.
2. Источники угроз информационной безопасности РФ. Информационная безопасность в условиях функционирования в России глобальных сетей. Виды противников или «нарушителей». Удаленные атаки на интрасети.

Задания для самостоятельной работы.

1. Что понимается под угрозой безопасности информации?
2. Перечислите и охарактеризуйте случайные угрозы.
3. Дайте общую характеристику преднамеренных угроз.
4. В чем состоит особенность определения несанкционированного доступа к информации?
5. Какие физические процессы лежат в основе появления побочных электромагнитных излучений и наводок?
6. Охарактеризуйте особенности угроз безопасности информации, связанных с несанкционированной модификацией структур КС.
7. Представьте классификацию видов возможных нарушений информационной системы.

Подготовьте рефераты по следующим темам:

1. Информационная безопасность в системе национальной безопасности РФ.
2. Компьютерные преступления.
3. Способы совершения компьютерных преступлений

Тема 2. Правовое обеспечение информационной безопасности

Лекция.

Основные нормативно-правовые акты в области информационной безопасности. Правовые особенности обеспечения безопасности конфиденциальной информации и государственной тайны. Законодательство в области лицензирования и сертификации. Правила функционирования системы лицензирования. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.

Практическое занятие.

1. Стандарты безопасности. Критерии безопасности компьютерных систем «Оранжевая книга».
2. Руководящие документы Гостехкомиссии

Задания для самостоятельной работы.

1. Защита информационных систем.
2. Критерии оценки процессов проектирования и правовой базы.
3. Особенности требований безопасности, отраженных в краткой спецификации в составе задания по безопасности.
4. Оценка создания более безопасных продуктов ИТ по направлениям.
5. Основные положения национальной безопасности страны.

Подготовьте рефераты по следующим темам:

1. Доктрина информационной безопасности РФ.
2. Правовая основа обеспечения информационной безопасности.
3. Конфиденциальная информация и государственная тайна. Правовые особенности их защиты.

Тема 3. Тема 3. Организационное обеспечение информационной безопасности. Механизмы обеспечения "информационной безопасности"

Лекция.

Основные стандарты в области обеспечения информационной безопасности. Политика безопасности. Экономическая безопасность предприятия. Виды угроз. Разграничение доступа к ресурсам ИС. Идентификация и аутентификация пользователей в ОС семейства Windows и Linux. Аудит событий безопасности. Администрирование прав пользователей. Аппаратно-программные комплексы обеспечения безопасности ОС. Основные виды сетевых и компьютерных угроз. Средства и методы защиты от сетевых компьютерных угроз.

Практическое занятие.

1. Виды угроз. Резервное копирование и восстановление данных. Разграничение доступа пользователей.
2. Права доступа в БД. Аудит в БД. Повышение надежности систем хранения данных. Сериализация транзакций. Журнализация.

Задания для самостоятельной работы.

1. Основные нормативные руководящие документы, касающиеся государственной тайны.
2. Нормативно-справочные документы.
3. Построение комплексных систем защиты информации.
4. Концепция создания защищенных КС.
5. Виды и способы защиты от проникновения в систему.
6. Программное обеспечение защиты компьютерных систем.
7. Организация функционирования комплексных систем защиты информации.
8. Информационная безопасность информационных систем.

Подготовьте рефераты по следующим темам:

1. Организационное обеспечение в системе обеспечения информационной безопасности.
2. Средства и методы защиты от сетевых компьютерных угроз.
3. Резервное копирование и восстановление данных.

Тест

1. Выберите правильный ответ

Как называется документ, который содержит официальные взгляды и цели государства в сфере информационной безопасности

- а) Конституция РФ
- б) Административный кодекс РФ
- в) Доктрина информационной безопасности РФ
- г) Уголовный кодекс РФ

2. Выберите правильный ответ

Комплекс действий, проводимых с целью подтверждения соответствия определенным нормам ГОСТ и других нормативных документов называется

- а) лицензированием
- б) сертификацией
- в) авторским правом
- г) торговой маркой

3. Выберите правильный ответ

В каком нормативно правовом акте можно найти санкции за преступлениями в сфере компьютерной информации?

- а) Конституция РФ
- б) Административный кодекс РФ

- в) Гражданский кодекс РФ
- г) Уголовный кодекс РФ

Тема 4. Тема 4. Программно-аппаратные средства и методы обеспечения информационной безопасности

Лекция.

Инженерная защита объектов. Защита информации от утечки по техническим каналам. Методы обеспечения информационной безопасности РФ. Ограничение доступа. Контроль доступа к аппаратуре. Разграничение и контроль доступа к информации. Предоставление привилегий на доступ. Ограничение доступа как метод обеспечения информационной безопасности. Биометрические методы аутентификации человека. Статистика применения биометрических технологий. Глаза, лицо, отпечатки пальцев и ладонь как биометрическая характеристика идентификации человека. Динамические характеристики как биометрическая характеристика идентификации человека. Разграничение и контроль доступа к информации как метод обеспечения информационной безопасности. Предоставление привилегий на доступ как метод обеспечения информационной безопасности.

Практическое занятие.

1. Идентификация и установление подлинности технических средств, подлинности документов, подлинности информации на средствах ее отображения и печати.
2. Защита информации от утечки за счет побочного электромагнитного излучения и наводок. Методы и средства защиты информации от побочного электромагнитного излучения и наводок информации.

Задания для самостоятельной работы.

1. Методы защиты информации, с использованием голографии.
2. Методы и средства шифрования и дешифровки.
3. Кодирования и средства защиты при шифровании данных.
4. Использование защищенных компьютерных систем.
5. Удаленный доступ к криптографическим защищенным файлам.
6. Методика защиты компьютерных систем.

Подготовьте рефераты по следующим темам:

1. Защита информации от утечки по техническим каналам.
2. Биометрические методы аутентификации человека.
3. Разграничение и контроль доступа к информации как метод обеспечения информационной безопасности.

Тема 5. Тема 5. Криптографические методы защиты информации

Лекция.

Методы криптографии. Классификация криптографических методов. Характеристики существующих шифров. Кодирование. Стеганография. Электронная подпись. Системы шифрования. Цифровые подписи (ЭЦП). ФЗ «Об электронной подписи».

Практическое занятие.

1. Классификация криптосистем. Симметричные криптосистемы. Классификация симметричных криптосистем. Шифрование методом замены (подстановки).
2. Характеристики существующих шифров. Основные правила криптозащиты.

Задания для самостоятельной работы.

1. Основные нормативные руководящие документы, касающиеся государственной тайны.
2. Нормативно-справочные документы.
3. Системы с закрытым и открытым ключом.
4. Модели безопасности и их применение.

5. Основные технологии построения защищенных ИС. Концепция информационной безопасности.
6. Основные технологии построения защищенных ИС.

Подготовьте рефераты по следующим темам:

1. Криптографические методы и средства защиты информации в компьютерных системах и сетях.
2. Основные технологии построения защищенных ИС.
3. Электронная подпись. (ЭП). Особенности её использования по законодательству РФ.

Тема 6. Тема 6. Компьютерные вирусы и методы антивирусной защиты. Информационная безопасность вычислительных сетей

Лекция.

Компьютерные вирусы и информационная безопасность. Характерные черты компьютерных вирусов. Классификация компьютерных вирусов. Антивирусные программы. Правила защиты от компьютерных вирусов.

Особенности обеспечения информационной безопасности в компьютерных сетях. Сетевые модели передачи данных. Адресация в глобальных сетях.

Условия существования вредоносных программ. Понятия о видах вирусов. Классические компьютерные вирусы. Сетевые черви. Троянские программы. Rootkit. Спам. Защита от компьютерных вирусов. Признаки заражения компьютера. Источники компьютерных вирусов. Основные правила защиты. Антивирусные программы.

Основные положения теории информационной безопасности информационных систем. Концепция информационной безопасности. Модели безопасности и их применение. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. Анализ способов нарушений информационной безопасности. Использование защищенных компьютерных систем.

Практическое занятие.

1. Классические компьютерные вирусы. Классификация классических вирусов. Способы заражения компьютерными вирусами
2. Сетевые черви. Троянские программы.
3. Хакерские утилиты и прочие вредоносные программы. Признаки заражения компьютера. Косвенные признаки заражения компьютера.

Задания для самостоятельной работы.

1. Понятия о видах вирусов.
2. Свойство вирусов.
3. Вредительские программы.
4. Способы защита от вирусов технические.
5. Способы защита от вирусов программные.
6. Вида возможных нарушений информационной системы.
7. Защита информационных систем.
8. Концепция информационной безопасности.

Подготовьте рефераты по следующим темам:

1. Компьютерные вирусы и антивирусные программы.
2. Политика и модели безопасности. Безопасность сетевых операционных систем.
3. Особенности обеспечения информационной безопасности в компьютерных сетях.

Тест

1. Выберите правильный ответ

Принципом политики информационной безопасности является принцип:

- а) усиления защищенности самого незащищенного звена сети (системы)
- б) перехода в безопасное состояние работы сети, системы
- в) полного доступа пользователей ко всем ресурсам сети, системы

2. Выберите правильный ответ

Как называется состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право?

- а) конфиденциальность
- б) доступность
- в) целостность

3. Выберите правильный ответ

Принципом политики информационной безопасности является принцип:

- а) разделения доступа (обязанностей, привилегий) клиентам сети (системы)
- б) одноуровневой защиты сети, системы
- в) совместимых, однотипных программно-технических средств сети, системы

4. Контроль знаний обучающихся и типовые оценочные средства

4.1. Распределение баллов:

3 семестр

- текущий контроль – 54 балла
- контрольные срезы – 2 среза по 8 баллов каждый
- премиальные баллы – 20 баллов
- ответ на экзамене: не более 30 баллов

Распределение баллов по заданиям:

№ темы	Название темы / вид учебной работы	Формы текущего контроля / срезы	Мак. кол-во баллов	Методика проведения занятия и оценки
1.	Тема 1. Введение в информационную безопасность	Опрос	3	<p>3 балла – студент умеет сопоставить полученную при подготовке к прак-тическому занятию информацию, сравнивать разные точки зрения на анализируемую проблему, уметь четко формулировать свои вопросы и отвечать на задаваемые ему вопро-сы.</p> <p>2 балла - студент умеет применять полученную при подготовке к прак-тическому занятию информацию, отвечать на большинство вопросов.</p> <p>1 балл – студент владеет теоретиче-ским материалом по теме практиче-ского занятия, иногда затрудняется при ответе на вопросы.</p> <p>Если студент не владеет проблема-тикой практического занятия, не мо-жет отвечать на вопросы, зачитывает ответ по напечатанному тексту – от-вет баллами не оценивается.</p>

		Реферат	6	<p>6 баллов – студент грамотно выстраивает логику своего доклада по материалам реферата, раскрывает тему исследования, опираясь на результаты теоретических и эмпирических исследований последних 3-5 лет, демонстрирует оригинальные находки в решении проблемы, намечены перспективы исследования, продемонстрированы хорошие ораторские способности, выступление сопровождается презентацией полученных результатов. Грамотные ответы на дополнительные вопросы</p> <p>5 баллов - студент грамотно выстраивает логику своего доклада по материалам реферата, раскрывает тему исследования, опираясь на результаты исследований последних 5 лет, демонстрирует отдельные оригинальные находки в решении проблемы, перспективы исследования намечены отдельными штрихами, продемонстрированы хорошие ораторские способности, выступление сопровождается презентацией полученных результатов. Даны грамотные ответы на отдельные дополнительные вопросы</p> <p>4 балла - логика выступления в отдельных местах нарушается, тема исследования раскрывается, опираясь на результаты исследований последних 10 лет, отсутствуют оригинальные находки в решении проблемы, перспективы исследования намечены пунктирно, продемонстрированы средние ораторские способности, выступление сопровождается презентацией полученных результатов, ответы на вопросы требуют уточнения.</p> <p>3 балла – представленные результаты в массе своей не новы, ответ представляет собой простое зачитывание текста, отдельные ответы на дополнительные вопросы требуют уточнения</p> <p>2 - 1 балл - представленные результаты в массе своей не новы, ответ представляет собой простое зачитывание текста, студент не может дать ответы на дополнительные вопросы</p>
2.	Тема 2. Правовое обеспечение информационной безопасности	Опрос	3	<p>3 балла – студент умеет сопоставить полученную при подготовке к практическому занятию информацию, сравнивать разные точки зрения на анализируемую проблему, уметь четко формулировать свои вопросы и отвечать на задаваемые ему вопросы.</p> <p>2 балла - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов.</p> <p>1 балл – студент владеет теоретическим материалом по теме практического занятия, иногда затрудняется при ответе на вопросы.</p> <p>Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается</p>

		Реферат	6	<p>6 баллов – студент грамотно выстраивает логику своего доклада по материалам реферата, раскрывает тему исследования, опираясь на результаты теоретических и эмпирических исследований последних 3-5 лет, демонстрирует оригинальные находки в решении проблемы, намечены перспективы исследования, продемонстрированы хорошие ораторские способности, выступление сопровождается презентацией полученных результатов. Грамотные ответы на дополнительные вопросы</p> <p>5 баллов - студент грамотно выстраивает логику своего доклада по материалам реферата, раскрывает тему исследования, опираясь на результаты исследований последних 5 лет, демонстрирует отдельные оригинальные находки в решении проблемы, перспективы исследования намечены отдельными штрихами, продемонстрированы хорошие ораторские способности, выступление сопровождается презентацией полученных результатов. Даны грамотные ответы на отдельные дополнительные вопросы</p> <p>4 балла - логика выступления в отдельных местах нарушается, тема исследования раскрывается, опираясь на результаты исследований последних 10 лет, отсутствуют оригинальные находки в решении проблемы, перспективы исследования намечены пунктирно, продемонстрированы средние ораторские способности, выступление сопровождается презентацией полученных результатов, ответы на вопросы требуют уточнения.</p> <p>3 балла – представленные результаты в массе своей не новы, ответ представляет собой простое зачитывание текста, отдельные ответы на дополнительные вопросы требуют уточнения</p> <p>2 - 1 балл - представленные результаты в массе своей не новы, ответ представляет собой простое зачитывание текста, студент не может дать ответы на дополнительные вопросы</p>
3.	Тема 3. Организационное обеспечение информационной безопасности. Механизмы обеспечения "информационной безопасности"	Опрос	3	<p>3 балла – студент умеет сопоставить полученную при подготовке к практическому занятию информацию, сравнивать разные точки зрения на анализируемую проблему, уметь четко формулировать свои вопросы и отвечать на задаваемые ему вопросы.</p> <p>2 балла - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов.</p> <p>1 балл – студент владеет теоретическим материалом по теме практического занятия, иногда затрудняется при ответе на вопросы.</p> <p>Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается</p>

		Реферат	6	<p>6 баллов – студент грамотно выстраивает логику своего доклада по материалам реферата, раскрывает тему исследования, опираясь на результаты теоретических и эмпирических исследований последних 3-5 лет, демонстрирует оригинальные находки в решении проблемы, намечены перспективы исследования, продемонстрированы хорошие ораторские способности, выступление сопровождается презентацией полученных результатов. Грамотные ответы на дополнительные вопросы</p> <p>5 баллов - студент грамотно выстраивает логику своего доклада по материалам реферата, раскрывает тему исследования, опираясь на результаты исследований последних 5 лет, демонстрирует отдельные оригинальные находки в решении проблемы, перспективы исследования намечены отдельными штрихами, продемонстрированы хорошие ораторские способности, выступление сопровождается презентацией полученных результатов. Даны грамотные ответы на отдельные дополнительные вопросы</p> <p>4 балла - логика выступления в отдельных местах нарушается, тема исследования раскрывается, опираясь на результаты исследований последних 10 лет, отсутствуют оригинальные находки в решении проблемы, перспективы исследования намечены пунктирно, продемонстрированы средние ораторские способности, выступление сопровождается презентацией полученных результатов, ответы на вопросы требуют уточнения.</p> <p>3 балла – представленные результаты в массе своей не новы, ответ представляет собой простое зачитывание текста, отдельные ответы на дополнительные вопросы требуют уточнения</p> <p>2 - 1 балл - представленные результаты в массе своей не новы, ответ представляет собой простое зачитывание текста, студент не может дать ответы на дополнительные вопросы</p>
		Тестирование(контрольный срез)	8	<p>8 - 6 баллов – студент правильно отвечает на 75-100% вопросов в тесте</p> <p>5 - 4 баллов – студент правильно отвечает на 50-74% вопросов в тесте</p> <p>3-1 балл – студент правильно отвечает на 25-50% вопросов в тесте.</p> <p>Менее 25% правильных ответов баллов не дает</p>
		Опрос	3	<p>3 балла – студент умеет сопоставить полученную при подготовке к практическому занятию информацию, сравнивать разные точки зрения на анализируемую проблему, уметь четко формулировать свои вопросы и отвечать на задаваемые ему вопросы.</p> <p>2 балла - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов.</p> <p>1 балл – студент владеет теоретическим материалом по теме практического занятия, иногда затрудняется при ответе на вопросы.</p> <p>Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается.</p>
4.	Тема 4. Программно-аппаратные средства и методы обеспечения информационной безопасности			

		Реферат	6	<p>6 баллов – студент грамотно выстраивает логику своего доклада по материалам реферата, раскрывает тему исследования, опираясь на результаты теоретических и эмпирических исследований последних 3-5 лет, демонстрирует оригинальные находки в решении проблемы, намечены перспективы исследования, продемонстрированы хорошие ораторские способности, выступление сопровождается презентацией полученных результатов. Грамотные ответы на дополнительные вопросы</p> <p>5 баллов - студент грамотно выстраивает логику своего доклада по материалам реферата, раскрывает тему исследования, опираясь на результаты исследований последних 5 лет, демонстрирует отдельные оригинальные находки в решении проблемы, перспективы исследования намечены отдельными штрихами, продемонстрированы хорошие ораторские способности, выступление сопровождается презентацией полученных результатов. Даны грамотные ответы на отдельные дополнительные вопросы</p> <p>4 балла - логика выступления в отдельных местах нарушается, тема исследования раскрывается, опираясь на результаты исследований последних 10 лет, отсутствуют оригинальные находки в решении проблемы, перспективы исследования намечены пунктирно, продемонстрированы средние ораторские способности, выступление сопровождается презентацией полученных результатов, ответы на вопросы требуют уточнения.</p> <p>3 балла – представленные результаты в массе своей не новы, ответ представляет собой простое зачитывание текста, отдельные ответы на дополнительные вопросы требуют уточнения</p> <p>2 - 1 балл - представленные результаты в массе своей не новы, ответ представляет собой простое зачитывание текста, студент не может дать ответы на дополнительные вопросы</p>
5.	Тема 5. Криптографические методы защиты информации	Опрос	3	<p>3 балла – студент умеет сопоставить полученную при подготовке к практическому занятию информацию, сравнивать разные точки зрения на анализируемую проблему, уметь четко формулировать свои вопросы и отвечать на задаваемые ему вопросы.</p> <p>2 балла - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов.</p> <p>1 балл – студент владеет теоретическим материалом по теме практического занятия, иногда затрудняется при ответе на вопросы.</p> <p>Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается.</p>

		Реферат	6	<p>6 баллов – студент грамотно выстраивает логику своего доклада по материалам реферата, раскрывает тему исследования, опираясь на результаты теоретических и эмпирических исследований последних 3-5 лет, демонстрирует оригинальные находки в решении проблемы, намечены перспективы исследования, продемонстрированы хорошие ораторские способности, выступление сопровождается презентацией полученных результатов. Грамотные ответы на дополнительные вопросы</p> <p>5 баллов - студент грамотно выстраивает логику своего доклада по материалам реферата, раскрывает тему исследования, опираясь на результаты исследований последних 5 лет, демонстрирует отдельные оригинальные находки в решении проблемы, перспективы исследования намечены отдельными штрихами, продемонстрированы хорошие ораторские способности, выступление сопровождается презентацией полученных результатов. Даны грамотные ответы на отдельные дополнительные вопросы</p> <p>4 балла - логика выступления в отдельных местах нарушается, тема исследования раскрывается, опираясь на результаты исследований последних 10 лет, отсутствуют оригинальные находки в решении проблемы, перспективы исследования намечены пунктирно, продемонстрированы средние ораторские способности, выступление сопровождается презентацией полученных результатов, ответы на вопросы требуют уточнения.</p> <p>3 балла – представленные результаты в массе своей не новы, ответ представляет собой простое зачитывание текста, отдельные ответы на дополнительные вопросы требуют уточнения</p> <p>2 - 1 балл - представленные результаты в массе своей не новы, ответ представляет собой простое зачитывание текста, студент не может дать ответы на дополнительные вопросы</p>
6.	Тема 6. Компьютерные вирусы и методы антивирусной защиты. Информационная безопасность вычислительных сетей	Опрос	3	<p>3 балла – студент умеет сопоставить полученную при подготовке к практическому занятию информацию, сравнивать разные точки зрения на анализируемую проблему, уметь четко формулировать свои вопросы и отвечать на задаваемые ему вопросы.</p> <p>2 балла - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов.</p> <p>1 балл – студент владеет теоретическим материалом по теме практического занятия, иногда затрудняется при ответе на вопросы.</p> <p>Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается.</p>

		Реферат	6	<p>6 баллов – студент грамотно выстраивает логику своего доклада по материалам реферата, раскрывает тему исследования, опираясь на результаты теоретических и эмпирических исследований последних 3-5 лет, демонстрирует оригинальные находки в решении проблемы, намечены перспективы исследования, продемонстрированы хорошие ораторские способности, выступление сопровождается презентацией полученных результатов. Грамотные ответы на дополнительные вопросы</p> <p>5 баллов - студент грамотно выстраивает логику своего доклада по материалам реферата, раскрывает тему исследования, опираясь на результаты исследований последних 5 лет, демонстрирует отдельные оригинальные находки в решении проблемы, перспективы исследования намечены отдельными штрихами, продемонстрированы хорошие ораторские способности, выступление сопровождается презентацией полученных результатов. Даны грамотные ответы на отдельные дополнительные вопросы</p> <p>4 балла - логика выступления в отдельных местах нарушается, тема исследования раскрывается, опираясь на результаты исследований последних 10 лет, отсутствуют оригинальные находки в решении проблемы, перспективы исследования намечены пунктирно, продемонстрированы средние ораторские способности, выступление сопровождается презентацией полученных результатов, ответы на вопросы требуют уточнения.</p> <p>3 балла – представленные результаты в массе своей не новы, ответ представляет собой простое зачитывание текста, отдельные ответы на дополнительные вопросы требуют уточнения</p> <p>2 - 1 балл - представленные результаты в массе своей не новы, ответ представляет собой простое зачитывание текста, студент не может дать ответы на дополнительные вопросы</p>
		Тестирование(контрольный срез)	8	<p>8 - 6 баллов – студент правильно отвечает на 75-100% вопросов в тесте</p> <p>5 - 4 баллов – студент правильно отвечает на 50-74% вопросов в тесте</p> <p>3-1 балл – студент правильно отвечает на 25-50% вопросов в тесте.</p> <p>Менее 25% правильных ответов баллов не дает</p>
7.	Премиальные баллы	20	Дополнительные премиальные баллы могут быть начислены:	<ul style="list-style-type: none"> - постоянная активность во время практических занятий – 10 баллов; - получение (или наличие) сертификата на умение работы с правовой ИПС «Гарант» или «Консультант Плюс» – 10 баллов; - полностью подготовленная к публикации статья по тематике в рамках дисциплины – 10 баллов; - выступление с докладом на конференции по тематике изучаемой дисциплины – 10 баллов; - помощь в организации мероприятий по тематике изучаемой дисциплины – 10 баллов; - публикация статьи по тематике изучаемой дисциплины в сборнике студенческих работ / материалах всероссийской конференции / журнале из перечня ВАК – 10 / 15 / 20
8.	Ответ на экзамене	30	10-17 баллов – студент раскрыл основные вопросы и задания билета на оценку «удовлетворительно» 18-24 баллов – студент раскрыл основные вопросы и задания билета на оценку «хорошо», 25-30 баллов – студент раскрыл основные вопросы и задания билета на оценку «отлично».	

9.	Индивидуальные задания, с помощью которых можно набрать дополнительные баллы на экзамене	50	Выполнение рефератов (0 - 10 баллов); аннотация статьи по тематике дисциплины (0 - 5 баллов); обзор законодательства по тематике дисциплины (0 - 15 баллов); обзор судебной практики по тематике дисциплины (0 - 20 баллов).
10.	Итого за семестр	100	

Итоговая оценка по экзамену выставляется в 100-балльной шкале и в традиционной четырехбалльной шкале. Перевод 100-балльной рейтинговой оценки по дисциплине в традиционную четырехбалльную осуществляется следующим образом:

100-балльная система	Традиционная система
85 - 100 баллов	Отлично
70 - 84 баллов	Хорошо
50 - 69 баллов	Удовлетворительно
Менее 50	Неудовлетворительно

4.2 Типовые оценочные средства текущего контроля

Опрос

Тема 1. Тема 1. Введение в информационную безопасность

Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:

- правильность ответа по содержанию;
- полнота и глубина ответа;
- сознательность ответа;
- логика изложения материала;
- рациональность использованных приемов и способов решения поставленной учебной задачи;
- своевременность и эффективность использования наглядных пособий и технических средств при ответе;
- использование дополнительного материала;
- рациональность использования времени, отведенного на задание

Тема 2. Тема 2. Правовое обеспечение информационной безопасности

Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:

- правильность ответа по содержанию;
- полнота и глубина ответа;
- сознательность ответа;
- логика изложения материала;
- рациональность использованных приемов и способов решения поставленной учебной задачи;
- своевременность и эффективность использования наглядных пособий и технических средств при ответе;
- использование дополнительного материала;
- рациональность использования времени, отведенного на задание.

Тема 3. Тема 3. Организационное обеспечение информационной безопасности. Механизмы обеспечения "информационной безопасности"

Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:

- правильность ответа по содержанию;
- полнота и глубина ответа;
- сознательность ответа;
- логика изложения материала;
- рациональность использованных приемов и способов решения поставленной учебной задачи;
- своевременность и эффективность использования наглядных пособий и технических средств при ответе;
- использование дополнительного материала;
- рациональность использования времени, отведенного на задание

Тема 4. Тема 4. Программно-аппаратные средства и методы обеспечения информационной безопасности

Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:

- правильность ответа по содержанию;
- полнота и глубина ответа;
- сознательность ответа;
- логика изложения материала;
- рациональность использованных приемов и способов решения поставленной учебной задачи;
- своевременность и эффективность использования наглядных пособий и технических средств при ответе;
- использование дополнительного материала;
- рациональность использования времени, отведенного на задание.

Тема 5. Тема 5. Криптографические методы защиты информации

Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:

- правильность ответа по содержанию;
- полнота и глубина ответа;
- сознательность ответа;
- логика изложения материала;
- рациональность использованных приемов и способов решения поставленной учебной задачи;
- своевременность и эффективность использования наглядных пособий и технических средств при ответе;
- использование дополнительного материала;
- рациональность использования времени, отведенного на задание.

Тема 6. Тема 6. Компьютерные вирусы и методы антивирусной защиты. Информационная безопасность вычислительных сетей

Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:

- правильность ответа по содержанию;
- полнота и глубина ответа;
- сознательность ответа;
- логика изложения материала;
- рациональность использованных приемов и способов решения поставленной учебной задачи;
- своевременность и эффективность использования наглядных пособий и технических средств при ответе;

- использование дополнительного материала;
- рациональность использования времени, отведенного на задание.

Реферат

Тема 1. Тема 1. Введение в информационную безопасность

Рефераты, доклады подготавливаются по актуальным вопросам изучаемой темы.

Реферат сосредоточен на принципиальных вопросах, таких как: актуальность рассматриваемой темы; новизна работы и основные выводы, сформулированные в ходе изучения материала.

Индивидуальная защита предполагает раскрытие личностного аспекта автора реферата в ходе работы над темой. Необходимо обосновать выбор темы и привести собственные методы и способы работы над проблемой, вынесенной в заглавие. Приведены оригинальные находки, собственные суждения, интересные факты и идеи, полученные в ходе разработки материала. В докладе должна быть отражена личностная значимость проделанной работы и намечены перспективы продолжения исследования. Возможны презентации, раздаточный материал, слайды и т.д.

Тема 2. Тема 2. Правовое обеспечение информационной безопасности

Рефераты, доклады подготавливаются по актуальным вопросам изучаемой темы.

Реферат сосредоточен на принципиальных вопросах, таких как: актуальность рассматриваемой темы; новизна работы и основные выводы, сформулированные в ходе изучения материала.

Индивидуальная защита предполагает раскрытие личностного аспекта автора реферата в ходе работы над темой. Необходимо обосновать выбор темы и привести собственные методы и способы работы над проблемой, вынесенной в заглавие. Приведены оригинальные находки, собственные суждения, интересные факты и идеи, полученные в ходе разработки материала. В докладе должна быть отражена личностная значимость проделанной работы и намечены перспективы продолжения исследования. Возможны презентации, раздаточный материал, слайды и т.д.

Тема 3. Тема 3. Организационное обеспечение информационной безопасности. Механизмы обеспечения "информационной безопасности"

Рефераты, доклады подготавливаются по актуальным вопросам изучаемой темы.

Реферат сосредоточен на принципиальных вопросах, таких как: актуальность рассматриваемой темы; новизна работы и основные выводы, сформулированные в ходе изучения материала.

Индивидуальная защита предполагает раскрытие личностного аспекта автора реферата в ходе работы над темой. Необходимо обосновать выбор темы и привести собственные методы и способы работы над проблемой, вынесенной в заглавие. Приведены оригинальные находки, собственные суждения, интересные факты и идеи, полученные в ходе разработки материала. В докладе должна быть отражена личностная значимость проделанной работы и намечены перспективы продолжения исследования. Возможны презентации, раздаточный материал, слайды и т.д.

Тема 4. Тема 4. Программно-аппаратные средства и методы обеспечения информационной безопасности

Рефераты, доклады подготавливаются по актуальным вопросам изучаемой темы.

Реферат сосредоточен на принципиальных вопросах, таких как: актуальность рассматриваемой темы; новизна работы и основные выводы, сформулированные в ходе изучения материала.

Индивидуальная защита предполагает раскрытие личностного аспекта автора реферата в ходе работы над темой. Необходимо обосновать выбор темы и привести собственные методы и способы работы над проблемой, вынесенной в заглавие. Приведены оригинальные находки, собственные суждения, интересные факты и идеи, полученные в ходе разработки материала. В докладе должна быть отражена личностная значимость проделанной работы и намечены перспективы продолжения исследования. Возможны презентации, раздаточный материал, слайды и т.д.

Тема 5. Тема 5. Криптографические методы защиты информации

Рефераты, доклады подготавливаются по актуальным вопросам изучаемой темы.

Реферат сосредоточен на принципиальных вопросах, таких как: актуальность рассматриваемой темы; новизна работы и основные выводы, сформулированные в ходе изучения материала.

Индивидуальная защита предполагает раскрытие личностного аспекта автора реферата в ходе работы над темой. Необходимо обосновать выбор темы и привести собственные методы и способы работы над проблемой, вынесенной в заглавие. Приведены оригинальные находки, собственные суждения, интересные факты и идеи, полученные в ходе разработки материала. В докладе должна быть отражена личностная значимость проделанной работы и намечены перспективы продолжения исследования. Возможны презентации, раздаточный материал, слайды и т.д.

Тема 6. Тема 6. Компьютерные вирусы и методы антивирусной защиты. Информационная безопасность вычислительных сетей

Рефераты, доклады подготавливаются по актуальным вопросам изучаемой темы.

Реферат сосредоточен на принципиальных вопросах, таких как: актуальность рассматриваемой темы; новизна работы и основные выводы, сформулированные в ходе изучения материала.

Индивидуальная защита предполагает раскрытие личностного аспекта автора реферата в ходе работы над темой. Необходимо обосновать выбор темы и привести собственные методы и способы работы над проблемой, вынесенной в заглавие. Приведены оригинальные находки, собственные суждения, интересные факты и идеи, полученные в ходе разработки материала. В докладе должна быть отражена личностная значимость проделанной работы и намечены перспективы продолжения исследования. Возможны презентации, раздаточный материал, слайды и т.д.

Тестирование

Тема 3. Тема 3. Организационное обеспечение информационной безопасности. Механизмы обеспечения "информационной безопасности"

Тест состоит из 15 вопросов.

Тема 6. Тема 6. Компьютерные вирусы и методы антивирусной защиты. Информационная безопасность вычислительных сетей

Тест состоит из 15 вопросов.

4.3 Промежуточная аттестация по дисциплине проводится в форме экзамена

Типовые вопросы экзамена (ОК-12, ПК-6, ПК-16)

1. Информационная безопасность как совокупность сбалансированных интересов личности, общества и государства.
2. Доктрина информационной безопасности Российской Федерации.
3. Виды угроз. Разграничение доступа к ресурсам ИС. Идентификация и аутентификация пользователей в ОС семейства Windows и Linux.
4. Аудит событий безопасности. Администрирование прав пользователей. Аппаратно-программные комплексы обеспечения безопасности ОС.
5. Классификация компьютерных преступлений. Способы совершения компьютерных преступлений.

Типовые задания для экзамена (ОК-12, ПК-6, ПК-16)

Типовые темы рефератов

1. Законодательство в области информационной безопасности
2. Информационная безопасность в системе национальной безопасности РФ
3. Криптографические методы и средства защиты информации в компьютерных системах и сетях

4. Политика и модели безопасности. Безопасность сетевых операционных систем
5. Особенности обеспечения информационной безопасности в компьютерных сетях.

Типовые вопросы теста

1. Выберите правильный ответ

Согласно статьи 24 Конституции РФ сбор, хранение, использование и распространение информации о частной жизни лица без его согласия

- а) возможны в исключительных случаях
- б) проводится постоянно
- в) не допускается

2. Выберите правильный ответ

Комплекс действий, проводимых с целью подтверждения соответствия определенным нормам ГОСТ и других нормативных документов называется

- а) лицензированием
- б) сертификацией
- в) авторским правом
- г) торговой маркой

3. Выберите правильный ответ

В каком нормативно правовом акте можно найти санкции за преступлениями в сфере компьютерной информации?

- а) Конституция РФ
- б) Административный кодекс РФ
- в) Гражданский кодекс РФ
- г) Уголовный кодекс РФ

4. Выберите правильный ответ

Как называется документ, который содержит официальные взгляды и цели государства в сфере информационной безопасности

- а) Конституция РФ
- б) Административный кодекс РФ
- в) Доктрина информационной безопасности РФ
- г) Уголовный кодекс РФ

5. Выберите правильный ответ

Основным нормативно-правовым документом, защищающим права, свободы и безопасность человека в системе информационных отношений, в РФ является

- а) Стратегия национальной безопасности РФ до 2020 года
- б) Конституция РФ
- в) ФЗ "О государственной тайне"
- г) Доктрина информационной безопасности РФ

4.4. Шкала оценивания промежуточной аттестации

Оценка	Компетенции	Дескрипторы (уровни) – основные признаки освоения (показатели достижения результата)
--------	-------------	--

«отлично» (85 - 100 баллов)	ОК-12	Обладает углубленными теоретическими знаниями в области информационной безопасности, основные инструментальные средства защиты информации; источники возникновения информационных угроз; модели и принципы защиты информации от несанкционированного доступа; методы антивирусной защиты информации; состав и методы организационно-правовой защиты информации, прослеживает междисциплинарные связи.¶Ответ построен логично, материал излагается четко, ясно, хорошим языком, аргументировано.¶
	ПК-6	Свободно ориентируется в способах защиты программного обеспечения от несанкционированного распространения и модификации; основах криптографических методов защиты информации; принципах проектирования защищенных баз данных, прослеживает междисциплинарные связи.¶Уверенно анализирует источники, риски и формы атак на информацию, правильно понимает угрозы, которыми подвергается информация, умеет управлять полномочиями и протоколами идентификации и аутентификации пользователей в СУБД и ОС.¶На вопросы отвечает кратко, аргументировано, уверенно, по существу.¶
	ПК-16	Обладает углубленными знаниями о методах взлома сетевых носителей и систем; классификации компьютерных вирусов, какую угрозу они представляют для безопасности информации и о правилах защиты от компьютерных вирусов и вредоносных программ; о нормах и требованиях Российского законодательства в области защиты информации.¶Свободно ориентируется в основных понятиях и определениях, используемых при изучении информационной безопасности; знает классификацию угроз информационной безопасности.¶Ответ построен логично, материал излагается четко, ясно, хорошим языком, аргументировано.¶
«хорошо» (70 - 84 баллов)	ОК-12	Демонстрирует достаточный уровень знаний в области информационной безопасности, основные инструментальные средства защиты информации; источники возникновения информационных угроз. ¶В основном знает модели и принципы защиты информации от несанкционированного доступа; методы антивирусной защиты информации; состав и методы организационно-правовой защиты информации, в отдельных примерах прослеживает междисциплинарные связи.¶Ответ построен логично, материал излагается хорошим языком.¶
	ПК-6	Достаточно хорошо ориентируется в способах защиты программного обеспечения от несанкционированного распространения и модификации; основах криптографических методов защиты информации; принципах проектирования защищенных баз данных, в отдельных примерах прослеживает междисциплинарные связи.¶В основном анализирует источники, риски и формы атак на информацию, в основном понимает угрозы, которыми подвергается информация, в отдельных примерах умеет управлять полномочиями и протоколами идентификации и аутентификации пользователей в СУБД и ОС. ¶Вопросы, задаваемые преподавателем, не вызывают существенных затруднений.¶

	ПК-16	Достаточно свободно ориентируется в методах взлома сетевых носителей и систем; в классификации компьютерных вирусов, какую угрозу они представляют для безопасности информации и о правилах защиты от компьютерных вирусов и вредоносных программ; о нормах и требованиях Российского законодательства в области защиты информации. ¶ В основном ориентируется в понятиях и определениях, используемых при изучении информационной безопасности; в основном знает классификацию угроз информационной безопасности. ¶ Ответ построен логично, материал излагается хорошим языком. ¶
«удовлетворительно» (50 - 69 баллов)	ОК-12	Демонстрирует недостаточный уровень знаний в области информационной безопасности, основные инструментальные средства защиты информации; источники возникновения информационных угроз. ¶ Плохо анализирует модели и принципы защиты информации от несанкционированного доступа; методы антивирусной защиты информации; состав и методы организационно-правовой защиты информации, не уверенно определяет междисциплинарные связи. ¶ Ответ не всегда логично выстроен, материал излагается без применения научной терминологии. ¶
	ПК-6	Слабо ориентируется в способах защиты программного обеспечения от несанкционированного распространения и модификации; основах криптографических методов защиты информации; принципах проектирования защищенных баз данных, не уверенно определяет междисциплинарные связи. ¶ Слабо анализирует источники, риски и формы атак на информацию, в основном понимает угрозы, которыми подвергается информация, не уверенно управляет полномочиями и протоколами идентификации и аутентификации пользователей в СУБД и ОС. ¶ Вопросы, задаваемые преподавателем, вызывают затруднения. ¶
	ПК-16	Слабо ориентируется в методах взлома сетевых носителей и систем; в классификации компьютерных вирусов, какую угрозу они представляют для безопасности информации и о правилах защиты от компьютерных вирусов и вредоносных программ; о нормах и требованиях Российского законодательства в области защиты информации. ¶ Слабо ориентируется в понятиях и определениях, используемых при изучении информационной безопасности; слабо знает классификацию угроз информационной безопасности. ¶ Ответ не всегда логично выстроен, материал излагается без применения научной терминологии. ¶
	ОК-12	Демонстрирует слабый уровень знаний в области информационной безопасности, основные инструментальные средства защиты информации; источники возникновения информационных угроз. ¶ Не может назвать модели и принципы защиты информации от несанкционированного доступа; методы антивирусной защиты информации; состав и методы организационно-правовой защиты информации, не определяет междисциплинарные связи. ¶ Неуверенно и логически непоследовательно излагает материал. ¶

«неудовлетворительно» (менее 50 баллов)	ПК-6	Не ориентируется в способах защиты программ-ного обеспечения от несанкционированного распро-странения и модификации; основах криптогра-фиче-ских методов защиты информации; принципах проектирования защищенных баз данных, не определяет междисциплинарные связи.¶Не анализирует источники, риски и формы атак на информацию, в основном понимает угрозы, которыми подвергается информация, не знает полномочий и протоколов идентификации и аутентификации пользователей в СУБД и ОС.¶Неправильно отвечает на поставленные вопросы или затрудняется с ответом.¶
	ПК-16	Не ориентируется в методах взлома сетевых носи-телей и систем; в классификации компьютерных ви-русов, какую угрозу они представляют для безопас-ности информации и о правилах защиты от компью-терных вирусов и вредоносных программ; о нормах и требованиях Российского законодательства в области защиты информации, не определяет междисципли-нарные связи. ¶Не ориентируется в понятиях и определениях, ис-пользуемых при изучении информационной безопас-ности; не знает классификацию угроз информаци-онной безопасности.¶Неуверенно и логически непоследовательно изла-гает материал.¶

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

5.1 Методические указания по организации самостоятельной работы обучающихся:

Приступая к изучению дисциплины, в первую очередь обучающимся необходимо ознакомиться содержанием рабочей программы дисциплины (РПД), которая определяет содержание, объем, а также порядок изучения и преподавания учебной дисциплины, ее раздела, части.

Для самостоятельной работы важное значение имеют разделы «Объем и содержание дисциплины», «Учебно-методическое и информационное обеспечение дисциплины» и «Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы».

В разделе «Объем и содержание дисциплины» указываются все разделы и темы изучаемой дисциплины, а также виды занятий и планируемый объем в академических часах.

В разделе «Учебно-методическое и информационное обеспечение дисциплины» указана рекомендуемая основная и дополнительная литература.

В разделе «Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы» содержится перечень профессиональных баз данных и информационных справочных систем, необходимых для освоения дисциплины.

5.2 Рекомендации обучающимся по работе с теоретическими материалами по дисциплине

При изучении и проработке теоретического материала необходимо:

- просмотреть еще раз презентацию лекции в системе MOODLe, повторить законспектированный на лекционном занятии материал и дополнить его с учетом рекомендованной дополнительной литературы;
- при самостоятельном изучении теоретической темы сделать конспект, используя рекомендованные в РПД источники, профессиональные базы данных и информационные справочные системы;
- ответить на вопросы для самостоятельной работы, по теме представленные в пункте 3.2 РПД.
- при подготовке к текущему контролю использовать материалы фонда оценочных средств (ФОС).

5.3 Рекомендации по работе с научной и учебной литературой

Работа с основной и дополнительной литературой является главной формой самостоятельной работы и необходима при подготовке к устному опросу на семинарских занятиях, к дебатам, тестированию, экзамену. Она включает проработку лекционного материала и рекомендованных источников и литературы по тематике лекций.

Конспект лекции должен содержать реферативную запись основных вопросов лекции, в том числе с опорой на размещенные в системе MOODLe презентации, основных источников и литературы по темам, выводы по каждому вопросу. Конспект может быть выполнен в рамках распечатки выдачи презентаций лекций или в отдельной тетради по предмету. Он должен быть аккуратным, хорошо читаемым, не содержать не относящуюся к теме информацию или рисунки.

Конспекты научной литературы при самостоятельной подготовке к занятиям должны содержать ответы на каждый поставленный в теме вопрос, иметь ссылку на источник информации с обязательным указанием автора, названия и года издания используемой научной литературы. Конспект может быть опорным (содержать лишь основные ключевые позиции), но при этом позволяющим дать полный ответ по вопросу, может быть подробным. Объем конспекта определяется самим студентом.

В процессе работы с основной и дополнительной литературой студент может:

- делать записи по ходу чтения в виде простого или развернутого плана (создавать перечень основных вопросов, рассмотренных в источнике);
- составлять тезисы (цитирование наиболее важных мест статьи или монографии, короткое изложение основных мыслей автора);
- готовить аннотации (краткое обобщение основных вопросов работы);
- создавать конспекты (развернутые тезисы).

5.4. Рекомендации по подготовке к отдельным заданиям текущего контроля

Собеседование предполагает организацию беседы преподавателя со студентами по вопросам практического занятия с целью более обстоятельного выявления их знаний по определенному разделу, теме, проблеме и т.п. Все члены группы могут участвовать в обсуждении, добавлять информацию, дискутировать, задавать вопросы и т.д.

Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:

- правильность ответа по содержанию;
- полнота и глубина ответа;
- сознательность ответа;
- логика изложения материала;
- рациональность использованных приемов и способов решения поставленной учебной задачи;
- своевременность и эффективность использования наглядных пособий и технических средств при ответе;
- использование дополнительного материала;
- рациональность использования времени, отведенного на задание.

Устный опрос может сопровождаться презентацией, которая подготавливается по одному из вопросов практического занятия. При выступлении с презентацией необходимо обращать внимание на такие моменты как:

- содержание презентации: актуальность темы, полнота ее раскрытия, смысловое содержание, соответствие заявленной темы содержанию, соответствие методическим требованиям (цели, ссылки на ресурсы, соответствие содержания и литературы), практическая направленность, соответствие содержания заявленной форме, адекватность использования технических средств учебным задачам, последовательность и логичность презентуемого материала;
- оформление презентации: объем (оптимальное количество), дизайн (читаемость, наличие и соответствие графики и анимации, звуковое оформление, структурирование информации, соответствие заявленным требованиям), оригинальность оформления, эстетика, использование возможности программной среды, соответствие стандартам оформления;
- личностные качества: ораторские способности, соблюдение регламента, эмоциональность, умение ответить на вопросы, систематизированные, глубокие и полные знания по всем разделам программы;

- содержание выступления: логичность изложения материала, раскрытие темы, доступность изложения, эффективность применения средств ИКТ, способы и условия достижения результативности и эффективности для выполнения задач своей профессиональной или учебной деятельности, доказательность принимаемых решений, умение аргументировать свои заключения, выводы.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Основная литература:

1. Федотов М. А., Антонова А. В., Будник Р. А., Войниканис Е. А., Околеснова О. А., Петрин И. В., Примакова А. В., Семенова Е. В., Тедеев А. А. Информационное право : Учебник для вузов. - Москва: Юрайт, 2020. - 497 с. - Текст : электронный // ЭБС «ЮРАЙТ» [сайт]. - URL: <https://urait.ru/bcode/451031>
2. Полякова Т. А., Чубукова С. Г., Ниесов В. А. Организационное и правовое обеспечение информационной безопасности : Учебник и практикум для вузов. - Москва: Юрайт, 2020. - 325 с. - Текст : электронный // ЭБС «ЮРАЙТ» [сайт]. - URL: <https://urait.ru/bcode/450371>

6.2 Дополнительная литература:

1. Рассолов И. М. Информационное право : Учебник и практикум для вузов. - пер. и доп; 5-е изд.. - Москва: Юрайт, 2020. - 347 с. - Текст : электронный // ЭБС «ЮРАЙТ» [сайт]. - URL: <https://urait.ru/bcode/449839>

6.3 Иные источники:

1. Библиотека научной и учебной литературы – <http://www.sbiblio.com> - <http://www.sbiblio.com>
2. Научно-практический журнал «Актуальные проблемы российского права» - <https://aprp.msaf.ru/jour/index> - <https://aprp.msaf.ru/jour/index>
3. Сайт «Российская газета»- <http://www.rg.ru> - <http://www.rg.ru>
4. Словари и энциклопедии онлайн - <http://dic.academic.ru/>
5. Федеральный научно-практический журнал «Юрист» - <http://lawinfo.ru/catalog/magazines/jurist/> - <http://lawinfo.ru/catalog/magazines/jurist/>

7. Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы

Для проведения занятий по дисциплине необходимо следующее материально-техническое обеспечение: учебные аудитории для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, помещения для самостоятельной работы.

Учебные аудитории и помещения для самостоятельной работы укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Помещения для самостоятельной работы укомплектованы компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Университета.

Для проведения занятий лекционного типа используются наборы демонстрационного оборудования, обеспечивающие тематические иллюстрации (проектор, ноутбук, экран/ интерактивная доска).

Лицензионное программное обеспечение:

Операционная система Microsoft Windows XP SP3

Операционная система "Альт Образование"

Электронный периодический справочник "Система ГАРАНТ"

Adobe Reader XI (11.0.08) - Russian Adobe Systems Incorporated 10.11.2014 187,00 MB 11.0.08

Kaspersky Endpoint Security для бизнеса - Стандартный Russian Edition. 1500-2499 Node 1 year Educational Renewal Licence

Консультант Плюс

7-Zip 9.20

ABBYY FineReader 8.0 Professional Edition

Профессиональные базы данных и информационные справочные системы:

1. Юрайт: электронно-библиотечная система. – URL: <https://urait.ru>
2. Электронный каталог Фундаментальной библиотеки ТГУ. – URL: <http://biblio.tsutmb.ru/elektronnyij-katalog>
3. Справочная правовая система "Консультант плюс". – URL: <http://www.consultant.ru>
4. Научная электронная библиотека eLIBRARY.ru. – URL: <https://elibrary.ru>

Электронная информационно-образовательная среда

https://auth.tsutmb.ru/authorize?response_type=code&client_id=moodle&state=xyz

Взаимодействие преподавателя и студента в процессе обучения осуществляется посредством мультимедийных, гипертекстовых, сетевых, телекоммуникационных технологий, используемых в электронной информационно-образовательной среде университета.