

Федеральное государственное бюджетное образовательное учреждение высшего образования «Тамбовский государственный университет имени Г.Р. Державина»
Институт экономики, информационных технологий и креативных индустрий
Кафедра математического моделирования и информационных технологий

УТВЕРЖДАЮ:
Директор института



Т. М. Кожевникова
«17» июня 2026 г.

РАБОЧАЯ ПРОГРАММА

по дисциплине Б1.В.3 Избранные вопросы информационной безопасности

Направление подготовки/специальность: 10.03.01 - Информационная безопасность

Профиль/направленность/специализация: Безопасность компьютерных систем

Уровень высшего образования: бакалавриат

Квалификация: Бакалавр

год набора: 2026

Автор программы:

Кандидат педагогических наук, доцент Анурьева Мария Сергеевна

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.03.01 - Информационная безопасность (уровень бакалавриата) (приказ Министерства науки и высшего образования РФ от «17» ноября 2020 г. № 1427).

Рабочая программа принята на заседании Кафедры математического моделирования и информационных технологий «16» июня 2026 г. Протокол № 11

Рассмотрена и одобрена на заседании Ученого совета Института экономики, информационных технологий и креативных индустрий, Протокол от «17» июня 2026 г. № 10.

СОДЕРЖАНИЕ

1. Цели и задачи дисциплины.....	4
2. Место дисциплины в структуре ОП бакалавриата.....	4
3. Объем и содержание дисциплины.....	4
4. Контроль знаний обучающихся и типовые оценочные средства.....	9
5. Методические указания для обучающихся по освоению дисциплины (модуля).....	48
6. Учебно-методическое и информационное обеспечение дисциплины.....	49
7. Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы.....	50

1. Цели и задачи дисциплины

1.1 Цель дисциплины – формирование компетенций:

ПК-3 Способен администрировать средства защиты информации прикладного и системного программного обеспечения

1.2 Типы задач профессиональной деятельности, к которым готовятся обучающиеся в рамках освоения дисциплины:

- эксплуатационный

1.3 Дисциплина ориентирована на подготовку обучающихся к профессиональной деятельности в сфере: 06 Связь, информационные и коммуникационные технологии (в сфере техники и технологии, охватывающей совокупность проблем, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере)

1.4 В результате освоения дисциплины у обучающихся должны быть сформированы:

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	Индикаторы достижения компетенций
	ПК-3 Способен администрировать средства защиты информации прикладного и системного программного обеспечения	Администрирует средства защиты информации прикладного и системного программного обеспечения, в том числе при решении избранных вопросов информационной безопасности

1.5 Согласование междисциплинарных связей дисциплин, обеспечивающих освоение компетенций:

ПК-3 Способен администрировать средства защиты информации прикладного и системного программного обеспечения

№ п/п	Наименование дисциплин, определяющих междисциплинарные связи	Форма обучения
		Очная (семестр)
		8
1	Преддипломная практика	+

2. Место дисциплины в структуре ОП бакалавриата:

Дисциплина «Избранные вопросы информационной безопасности» относится к части, формируемой участниками образовательных отношений, учебного плана ОП по направлению подготовки 10.03.01 - Информационная безопасность.

Дисциплина «Избранные вопросы информационной безопасности» изучается в 7, 8 семестрах.

3. Объем и содержание дисциплины

3.1. Объем дисциплины: 5 з.е.

Очная: 5 з.е.

Вид учебной работы	Очная (всего часов)
Общая трудоёмкость дисциплины	180
Контактная работа	84
Лекции (Лекции)	32
Практические (Практ. раб.)	52
Самостоятельная работа (СР)	60
Экзамен	36
Зачет	-

3.2.Содержание курса:

№ темы	Название раздела/темы	Вид учебной работы, час.			Формы текущего контроля
		Лек ции	Пра кт. раб.	СР	
		О	О	О	
8 семестр					
1	Информация как объект правового регулирования.	1	-	1	Собеседование; Тестирование
2	Законодательство РФ в области информационной безопасности.	1	-	1	Собеседование; Тестирование
3	Правовые режимы защиты конфиденциальной информации.	2	-	2	Собеседование; Тестирование
4	Лицензирование и сертификация в информационной сфере.	2	-	2	Собеседование; Тестирование
5	Компьютерные правонарушения.	2	-	2	Собеседование; Тестирование
6	Внутренние нормативные документы по ИБ.	2	-	2	Собеседование; Тестирование
7	Угрозы. Система управления информационной безопасностью предприятия.	2	-	2	Собеседование; Тестирование

8	Математическое моделирование, программная реализация и анализ протоколов безопасной передачи данных как динамических систем.	2	-	2	Собеседование; Тестирование
9	Организация технической защиты информации.	2	-	2	Собеседование; Тестирование
10	Интеллектуальная собственность и ее защита.	2	-	2	Собеседование; Тестирование
11	Информационно-аналитическое обеспечение правоохранительной деятельности.	2	-	2	Собеседование; Тестирование
12	Информационно-психологическое обеспечение правоохранительной деятельности.	2	-	2	Собеседование; Тестирование
13	Организационная защита информации.	2	-	2	Собеседование; Защита лабораторной работы ; Тестирование

Тема 1. Информация как объект правового регулирования. (ПК-3)

Лекция.

Правовой режим. Понятие информации. Документированная информация. Целостность, конфиденциальность и доступность информации. Виды тайн. Собственник, владелец и пользователь информации.

Задания для самостоятельной работы.

- подготовка к лекциям, повторение учебного материала предыдущих лекций;
- изучение материалов лекционного курса по заданиям на самостоятельную проработку, выдаваемых преподавателем на занятиях.

Тема 2. Законодательство РФ в области информационной безопасности. (ПК-3)

Лекция.

Доктрина информационной безопасности Российской Федерации. Стратегия национальной безопасности Российской Федерации до 2020 года. Федеральный закон «О государственной тайне». Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера». Нормативные правовые акты ФСТЭК и ФСБ РФ.

Задания для самостоятельной работы.

- подготовка к лекциям, повторение учебного материала предыдущих лекций;

- изучение материалов лекционного курса по заданиям на самостоятельную проработку, выдаваемых преподавателем на занятиях.

Тема 3. Правовые режимы защиты конфиденциальной информации. (ПК-3)

Лекция.

Конфиденциальная информация: понятие, признаки, классификация. Административно-правовые отношения по поводу конфиденциальной информации. Структура административно-правовых режимов конфиденциальной информации. Административно-правовой режим персональных данных. Административно-правовой режим служебной тайны. Административно-правовой режим коммерческой тайны.

Задания для самостоятельной работы.

- подготовка к лекциям, повторение учебного материала предыдущих лекций;
- изучение материалов лекционного курса по заданиям на самостоятельную проработку, выдаваемых преподавателем на занятиях.

Тема 4. Лицензирование и сертификация в информационной сфере. (ПК-3)

Лекция.

Понятия лицензирования и сертификации. Нормативные и правовые документы в области лицензирования и сертификации. Органы лицензирования.

Задания для самостоятельной работы.

- подготовка к лекциям, повторение учебного материала предыдущих лекций;
- изучение материалов лекционного курса по заданиям на самостоятельную проработку, выдаваемых преподавателем на занятиях.

Тема 5. Компьютерные правонарушения. (ПК-3)

Лекция.

Понятие компьютерных преступлений. Неправомерный доступ к компьютерной информации. Создание, использование и распространение вредоносных программ. Нарушение правил эксплуатации.

Задания для самостоятельной работы.

- подготовка к лекциям, повторение учебного материала предыдущих лекций;
- изучение материалов лекционного курса по заданиям на самостоятельную проработку, выдаваемых преподавателем на занятиях.

Тема 6. Внутренние нормативные документы по ИБ. (ПК-3)

Лекция.

Концепция обеспечения информационной безопасности. Политика ИБ. Обязательство о неразглашении защищаемых сведений. Перечень защищаемых сведений. Положение о работе с защищаемыми сведениями.

Задания для самостоятельной работы.

- подготовка к лекциям, повторение учебного материала предыдущих лекций;
- изучение материалов лекционного курса по заданиям на самостоятельную проработку, выдаваемых преподавателем на занятиях.

Тема 7. Угрозы. Система управления информационной безопасностью предприятия. (ПК-3)

Лекция.

Основные функции систем управления информационной безопасностью. Принципы управления информационной безопасностью. Понятие риска. Идентификация рисков. Оценка вероятности реализации угроз. Оценивание рисков. Измерение рисков. Допустимый уровень риска.

Задания для самостоятельной работы.

- подготовка к лекциям, повторение учебного материала предыдущих лекций;

- изучение материалов лекционного курса по заданиям на самостоятельную проработку, выдаваемых преподавателем на занятиях.

Тема 8. Математическое моделирование, программная реализация и анализ протоколов безопасной передачи данных как динамических систем. (ПК-3)

Лекция.

Теоретические основы динамических систем и протоколов безопасности. Инструментарий для моделирования в Python. Моделирование базовых криптографических примитивов. Моделирование протоколов с симметричным ключом. Моделирование протоколов с асимметричным ключом. Моделирование сложных протоколов и анализ устойчивости.

Задания для самостоятельной работы.

- подготовка к лекциям, повторение учебного материала предыдущих лекций;
- изучение материалов лекционного курса по заданиям на самостоятельную проработку, выдаваемых преподавателем на занятиях.

Тема 9. Организация технической защиты информации. (ПК-3)

Лекция.

Общие положения по инженерно-технической защите информации в организации. Краткая характеристика государственной системы защиты информации. Основные руководящие и нормативные документы по организации инженерно-технической защиты информации в организации, их сущность. Организационные и технические меры по инженерно-технической защите информации в организации. Задачи и виды контроля эффективности защиты информации.

Задания для самостоятельной работы.

- подготовка к практическим занятиям, повторение изучения лекционного материала;
- подготовка к лекциям, повторение учебного материала предыдущих лекций;
- изучение материалов лекционного курса по заданиям на самостоятельную проработку, выдаваемых преподавателем на занятиях.

Тема 10. Интеллектуальная собственность и ее защита. (ПК-3)

Лекция.

Понятие интеллектуальной собственности, ее виды. Интеллектуальный продукт как объект интеллектуальной собственности и предмет защиты. Содержание гражданско-правовых норм в области защиты интеллектуальной собственности. Авторское право. Патентное право. Товарный знак. Договорное право, авторские и лицензионные договоры.

Задания для самостоятельной работы.

- подготовка к практическим занятиям, повторение изучения лекционного материала;
- подготовка к лекциям, повторение учебного материала предыдущих лекций;
- изучение материалов лекционного курса по заданиям на самостоятельную проработку, выдаваемых преподавателем на занятиях.

Тема 11. Информационно-аналитическое обеспечение правоохранительной деятельности. (ПК-3)

Лекция.

Понятие, сущность, задачи информационно-аналитического обеспечения правоохранительной деятельности. Методика информационно-аналитической работы. Основа работы с информацией. Основные свойства и возможности юридических информационных систем. Содержание аналитической деятельности. Информационно-аналитические технологии в аналитической деятельности. Представление результатов аналитической деятельности. Информационно-аналитическое обеспечение организационно-управленческой деятельности в правоохранительных органах. Информационно-аналитическое обеспечение оперативно-розыскной деятельности в правоохранительных органах. Информационно-аналитическое обеспечение раскрытия и расследования преступлений.

Задания для самостоятельной работы.

- подготовка к практическим занятиям, повторение изучения лекционного материала;
- подготовка к лекциям, повторение учебного материала предыдущих лекций;
- изучение материалов лекционного курса по заданиям на самостоятельную проработку, выдаваемых преподавателем на занятиях.

Тема 12. Информационно-психологическое обеспечение правоохранительной деятельности. (ПК-3)

Лекция.

Психологические аспекты формирования профессиональных качеств сотрудника. Основные задачи психологической подготовки. Формирование психологической готовности к борьбе с преступностью. Психологические особенности сотрудников правоохранительной сферы. Психологические особенности деятельности сотрудников. Психологические особенности личности сотрудника органов внутренних дел. Психологическая подготовка сотрудников органов внутренних дел.

Задания для самостоятельной работы.

- подготовка к практическим занятиям, повторение изучения лекционного материала;
- подготовка к лекциям, повторение учебного материала предыдущих лекций;
- изучение материалов лекционного курса по заданиям на самостоятельную проработку, выдаваемых преподавателем на занятиях.

Тема 13. Организационная защита информации. (ПК-3)

Лекция.

Концептуальные положения организационного обеспечения информационной безопасности. Организация службы безопасности объекта. Функции, задачи и особенности службы безопасности объекта. Организация внутриобъектового режима. Организация аналитической работы по предупреждению утечки конфиденциальной информации. Защита информации при проведении совещаний и переговоров. Работа с кадрами, владеющие конфиденциальной информацией. Методы обеспечения информационной безопасности российской федерации. Организация охраны объектов. Цели и задачи, объекты, виды и способы охраны. Классификация информационных ресурсов.

Задания для самостоятельной работы.

- подготовка к практическим занятиям, повторение изучения лекционного материала;
- подготовка к лекциям, повторение учебного материала предыдущих лекций;
- изучение материалов лекционного курса по заданиям на самостоятельную проработку, выдаваемых преподавателем на занятиях.

4. Контроль знаний обучающихся и типовые оценочные средства

4.1. Распределение баллов:

8 семестр

- посещаемость – 10 баллов
- текущий контроль – 80 баллов

- контрольные срезы – 2 среза по 5 баллов каждый
- премиальные баллы – 20 баллов

Распределение баллов по заданиям:

№ те мы	Название темы / вид учебной работы	Формы текущего контроля / срезы	Мах. кол-во баллов	Методика проведения занятия и оценки
1.	Информация как объект правового регулирования.	Собеседование	5	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. 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. 5 баллов - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию . Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается
		Тестирование	5	Оценка теста по текущему разделу или теме дисциплины 5 баллов – студент правильно отвечает на 50-100% вопросов в тесте. 0 баллов - студент правильно отвечает на 25-50% вопросов в тесте

2.	Законодательств во РФ в области информационн ой безопасности.	Собеседо вание	5	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. 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. 5 баллов - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию . Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается
		Тестиров ание	5	Оценка теста по текущему разделу или теме дисциплины 5 баллов – студент правильно отвечает на 50-100% вопросов в тесте. 0 баллов - студент правильно отвечает на 25-50% вопросов в тесте
3.	Правовые режимы защиты конфиденциаль ной информации.	Собеседо вание(ко нтрольн ый срез)	5	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. 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. 5 баллов - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию . Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается
		Тестиров ание	5	Оценка теста по текущему разделу или теме дисциплины 5 баллов – студент правильно отвечает на 50-100% вопросов в тесте. 0 баллов - студент правильно отвечает на 25-50% вопросов в тесте

4.	Лицензировани е и сертификация в информационн ой сфере.	Собеседо вание	5	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. 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. 5 баллов - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию . Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается
		Тестиров ание	5	Оценка теста по текущему разделу или теме дисциплины 5 баллов – студент правильно отвечает на 50-100% вопросов в тесте. 0 баллов - студент правильно отвечает на 25-50% вопросов в тесте
5.	Компьютерные правонарушени я.	Собеседо вание	5	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. 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. 5 баллов - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию . Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается
		Тестиров ание	5	Оценка теста по текущему разделу или теме дисциплины 5 баллов – студент правильно отвечает на 50-100% вопросов в тесте. 0 баллов - студент правильно отвечает на 25-50% вопросов в тесте

6.	Внутренние нормативные документы по ИБ.	Собеседование	5	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. 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. 1 балл - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию . Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается
		Тестирование	5	Оценка теста по текущему разделу или теме дисциплины 5 баллов – студент правильно отвечает на 50-100% вопросов в тесте. 0 баллов - студент правильно отвечает на 25-50% вопросов в тесте
7.	Угрозы. Система управления информационной безопасностью предприятия.	Собеседование	5	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. 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. 5 баллов - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию . Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается
		Тестирование(контрольный срез)	5	Оценка теста по текущему разделу или теме дисциплины 5 баллов – студент правильно отвечает на 50-100% вопросов в тесте. 0 баллов - студент правильно отвечает на 25-50% вопросов в тесте

8.	Математическое моделирование, программная реализация и анализ протоколов безопасной передачи данных как динамических систем.	Собеседование	1	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. 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. 1 балл - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию. Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается
		Тестирование	5	Оценка теста по текущему разделу или теме дисциплины 3 балла – студент правильно отвечает на 50-100% вопросов в тесте. 0 баллов - студент правильно отвечает на 25-50% вопросов в тесте
9.	Организация технической защиты информации.	Собеседование	1	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. 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. 1 балл - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию. Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается
		Тестирование	3	Оценка теста по текущему разделу или теме дисциплины 3 балла – студент правильно отвечает на 50-100% вопросов в тесте. 0 баллов - студент правильно отвечает на 25-50% вопросов в тесте.

10.	Интеллектуальная собственность и ее защита.	Собеседование	1	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. 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. 1 балл - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию . Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается
		Тестирование	1	Оценка теста по текущему разделу или теме дисциплины 1 балл – студент правильно отвечает на 50-100% вопросов в тесте. 0 баллов - студент правильно отвечает на 25-50% вопросов в тесте.
11.	Информационное обеспечение правоохранительной деятельности.	Собеседование	1	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. 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. 1 балл - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию . Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается
		Тестирование	1	Оценка теста по текущему разделу или теме дисциплины 1 балл – студент правильно отвечает на 50-100% вопросов в тесте. 0 баллов - студент правильно отвечает на 25-50% вопросов в тесте.

12.	Информационно-психологическое обеспечение правоохранительной деятельности.	Собеседование	1	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. 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. 1 балл - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию . Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается
		Тестирование	1	Оценка теста по текущему разделу или теме дисциплины 1 балл – студент правильно отвечает на 50-100% вопросов в тесте. 0 баллов - студент правильно отвечает на 25-50% вопросов в тесте.
13.	Организационная защита информации.	Собеседование	1	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. 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. 1 балл - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию . Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается

	Защита лабораторной работы	2	Лабораторные работы выполняются по текущему разделу или теме дисциплины. 2 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы, используя профессиональную терминологию. 1 балл - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенные ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы.
	Тестирование	1	Оценка теста по текущему разделу или теме дисциплины 1 балл – студент правильно отвечает на 50-100% вопросов в тесте. 0 баллов - студент правильно отвечает на 25-50% вопросов в тесте.
14.	Посещаемость	10	10 баллов – студент посетил все 100% занятий 7-9 баллов – студент посетил не менее 80% занятий 4-6 баллов – студент посетил не менее 50% занятий 1-3 балла – студент посетил не менее 25% занятий Если студент посетил менее 25% занятий, баллы не начисляются
15.	Премияльные баллы	20	Дополнительные премияльные баллы могут быть начислены: - за проект, выполненный по заказу работодателя и реализованный на практике – 20 баллов; - постоянная активность во время практических занятий – 10 баллов; - полностью подготовленная к публикации статья по тематике в рамках дисциплины – 10 баллов; - участие с докладом во всероссийской олимпиаде по тематике изучаемой дисциплины – 20 баллов; - участие в выставке по тематике изучаемой дисциплины – 20 баллов; - публикация статьи по тематике изучаемой дисциплины в сборнике студенческих работ / материалах всероссийской конференции / журнале из перечня ВАК – 10 / 15 / 20
16.	Индивидуальные задания, с помощью которых можно набрать дополнительные баллы	20	Решение кейса (10 баллов) Прохождение тестирования (30 вопросов) по всему курсу дисциплины (10 баллов)
17.	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

Защита лабораторной работы

Тема 13. Организационная защита информации.

Понятие целостности данных и

аутентификации источника данных. Задачи защиты информации, решаемые с помощью электронной подписи. Понятие о проверке электронной подписи. Пример реализации ЭП с помощью криптосистемы Эль-Гамала. Понятие о проверке электронной подписи.

Собеседование

Тема 1. Информация как объект правового регулирования.

1. Какие подходы существуют в определении понятия информации?
2. Что такое документированная информация?
3. Что такое целостность, конфиденциальность и доступность информации?
4. Какие виды тайн существуют в РФ?
5. В чем различие понятий собственник, владелец и пользователь информации?

Тема 2. Законодательство РФ в области информационной безопасности.

1. Что представляет собой доктрина информационной безопасности РФ?
2. Что представляет собой стратегия информационной безопасности РФ до 2020 года?
3. Какие виды отношений регулирует федеральный закон «О государственной тайне»?
4. Какие виды отношений регулирует федеральный закон «Об информации, информационных технологиях и о защите информации»?
5. Какие нормативные акты ФСЭК и ФСБ РФ вы знаете?

Тема 3. Правовые режимы защиты конфиденциальной информации.

1. Что такое конфиденциальная информация?
2. Какие виды сведений конфиденциального характера вы знаете?
3. Какой основной закон регулирует административно-правовые отношения по поводу конфиденциальной информации?
4. Что такое персональные данные и почему необходимо их защищать?
5. Какую информацию можно отнести к служебной тайне?

Тема 4. Лицензирование и сертификация в информационной сфере.

1. Что называется лицензированием?
2. Что такое лицензия?
3. Дайте определение сертификации?
4. Что входит в организационную структуру системы лицензирования?
5. Перечислите нормативные и правовые документы в области лицензирования и сертификации.
6. Приведите пример органов лицензирования.

Тема 5. Компьютерные правонарушения.

1. Что такое компьютерные преступления?
2. В чём заключается несанкционированный доступ к информации?
3. Перечислите причины несанкционированного доступа.
4. Какие программы называются вредоносными?
5. Приведите основные типы вредоносных программ.
6. Расскажите классификацию вредоносных программ.
7. Какое наказание грозит за неправомерный доступ к компьютерной информации?
8. Перечислите наказания предусмотренные за создание и распространение вредоносных программ.
9. Какие наказания предусмотрены Ст. 274 Уголовного кодекса РФ?

Тема 6. Внутренние нормативные документы по ИБ.

1. Что определяет концепция обеспечения информационной безопасности?
2. Что такое политика ИБ и каково ее назначение?
3. Какие пункты содержит «Обязательство о неразглашении конфиденциальной информации»?
4. Какие сведения можно включить в «Перечень сведений конфиденциального характера»?
5. С какой целью разрабатывается «Положение о работе с защищаемыми сведениями»?

Тема 7. Угрозы. Система управления информационной безопасностью предприятия.

1. На основании положений каких международных стандартов должно осуществляться построение СУИБ?
2. Назовите три основные функции СУИБ.
3. Какова цель применения процессного подхода как одного из принципов управления ИБ?
4. Назовите этапы процесса оценки рисков ИБ.
5. Объясните цель и механизм применения количественного и качественного подхода к оценке рисков ИБ.

Тема 8. Математическое моделирование, программная реализация и анализ протоколов безопасной передачи данных как динамических систем.

1. Опишите механизм следообразования в компьютерных системах?
2. Какие возможности исследования следов в компьютерных системах?
3. Как восстанавливать удаленную информацию?
4. Какой порядок действия по организации и проведению расследования компьютерных инцидентов?
5. Какой инструментальный используется при компьютерном исследовании?

Тема 9. Организация технической защиты информации.

1. Каким федеральным законом РФ установлено понятие термина «информация»?
2. Какие сведения относятся к государственной тайне?
3. Какая информация является признаковой?
4. Что такое прямые и косвенные демаскирующие признаки?
5. Что такое опасный сигнал?

Тема 10. Интеллектуальная собственность и ее защита.

1. Какие выделяют принципы защиты информации?
2. Что и кто обеспечивает функционирование государственной системы защиты информации?
3. Назовите основные руководящие документы по защите информации?
4. Какие выделяют организационные и технические меры по защите информации?
5. Назовите виды контроля защиты информации

Тема 11. Информационно-аналитическое обеспечение правоохранительной деятельности.

1. В чем отличие авторского от патентного права?
2. Какие виды интеллектуальной собственности существуют?
3. Что такое «интеллектуальный продукт»?
4. В чем особенность договорного права?
5. Какое содержание гражданско-правовых норм в области защиты интеллектуальной собственности?
6. Что общего между авторским и лицензионным договором?

Тема 12. Информационно-психологическое обеспечение правоохранительной деятельности.

1. Информационное обеспечение правоохранительных органов.
2. Информационные технологии правоохранительной деятельности.
3. Правовые автоматизированные системы учета и управления.

4. Правовые автоматизированные информационные системы.
5. Правовые автоматизированные информационно-справочные

Тема 13. Организационная защита информации.

1. Понятие информации и коммуникация.
2. Свойства информации.
3. Задачи информационно-психологической безопасности.
4. Угрозы информационно-психологической безопасности личности.
5. Средства информационно-психологического воздействия

Тестирование

Тема 1. Информация как объект правового регулирования.

1. Информация это -
 - 1 а. сведения, поступающие от СМИ
 - 2 б. только документированные сведения о лицах, предметах, фактах, событиях
 - 3 с. сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления
 - 4 д. только сведения, содержащиеся в электронных базах данных
2. Информация
 - 1 а. не исчезает при потреблении
 - 2 б. становится доступной, если она содержится на материальном носителе
 - 3 с. подвергается только "моральному износу"
 - 4 д. характеризуется всеми перечисленными свойствами
3. Информация, зафиксированная на материальном носителе, с реквизитами,
 - 1 а. позволяющими ее идентифицировать, называется
 - 2 а. достоверной
 - 3 б. конфиденциальной
 - 4 с. документированной
 - 5 д. коммерческой тайной
4. Формы защиты интеллектуальной собственности -
 - 1 а. авторское, патентное право и коммерческая тайна
 - 2 б. интеллектуальное право и смежные права
 - 3 с. коммерческая и государственная тайна
 - 4 д. гражданское и административное право
5. По принадлежности информационные ресурсы подразделяются на
 - 1 а. государственные, коммерческие и личные
 - 2 б. государственные, не государственные и информацию о гражданах
 - 3 с. информацию юридических и физических лиц
 - 4 д. официальные, гражданские и коммерческие
6. К негосударственным относятся информационные ресурсы
 - 1 а. созданные, приобретенные за счет негосударственных учреждений и организаций
 - 2 б. созданные, приобретенные за счет негосударственных предприятий и физических лиц
 - 3 с. полученные в результате дарения юридическими или физическими лицами

указанные в п.1-3

7. По доступности информация классифицируется на
 - 1 а. открытую информацию и государственную тайну
 - 2 б. конфиденциальную информацию и информацию свободного доступа
 - 3 с. информацию с ограниченным доступом и общедоступную информацию
 - 4 d. виды информации, указанные в остальных пунктах
8. К конфиденциальной информации относятся документы, содержащие
 - 1 а. государственную тайну
 - 2 б. законодательные акты
 - 3 с. "ноу-хау"
 - 4 d. сведения о золотом запасе страны
9. Запрещено относить к информации ограниченного доступа:
 - 1 а. информацию о чрезвычайных ситуациях
 - 2 б. информацию о деятельности органов государственной власти
 - 3 с. документы открытых архивов и библиотек
 - 4 d. все, перечисленное в остальных пунктах

Тема 2. Законодательство РФ в области информационной безопасности.

1. К конфиденциальной информации не относится
 - 1 а. коммерческая тайна
 - 2 б. персональные данные о гражданах
 - 3 с. государственная тайна
 - 4 d. "ноу-хау"
2. Вопросы информационного обмена регулируются (...) правом
 - 1 а. гражданским
 - 2 б. информационным
 - 3 с. конституционным
 - 4 d. уголовным
3. Согласно ст.132 ГК РФ интеллектуальная собственность это
 - 1 а. информация, полученная в результате интеллектуальной деятельности индивида
 - 2 б. литературные, художественные и научные произведения
 - 3 с. изобретения, открытия, промышленные образцы и товарные знаки
 - 4 d. исключительное право гражданина или юридического лица на результаты
 - 5 б. интеллектуальной деятельности
4. Интеллектуальная собственность включает права, относящиеся к
 - 1 а. литературным, художественным и научным произведениям, изобретениям и
 - 2 б. открытиям
 - 3 а. исполнительской деятельности артиста, звукозаписи, радио- и телепередачам
 - 4 б. промышленным образцам, товарным знакам, знакам обслуживания, фирменным
 - 5 с. наименованиям и коммерческим обозначениям
 - 6 а. всему, указанному в остальных пунктах

5. Конфиденциальная информация это

- 1 а. сведения, составляющие государственную тайну
- 2 б. сведения о состоянии здоровья высших должностных лиц
- 3 с. документированная информация, доступ к которой ограничивается в
- 4 б. соответствии с законодательством РФ
- 5 а. данные о состоянии преступности в стране

6. Какая информация подлежит защите?

- 1 а. информация, циркулирующая в системах и сетях связи
- 2 б. зафиксированная на материальном носителе информация с реквизитами,
- 3 б. позволяющими ее идентифицировать
- 4 а. только информация, составляющая государственные информационные ресурсы
- 5 б. любая документированная информация, неправомерное обращение с которой
- 6 с. может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу

7. Система защиты государственных секретов определяется Законом

- 1 а. "Об информации, информатизации и защите информации"
- 2 б. "Об органах ФСБ"
- 3 с. "О государственной тайне"
- 4 d. "О безопасности"

8. Государственные информационные ресурсы не могут принадлежать

- 1 а. физическим лицам
- 2 б. коммерческим предприятиям
- 3 с. негосударственным учреждениям
- 4 d. всем перечисленным субъектам

9. Из нижеперечисленных законодательных актов наибольшей юридической силой в вопросах информационного права обладает

- 1 а. Указ Президента "Об утверждении перечня сведений, относящихся к
- 2 б. государственной тайне"
- 3 а. ГК РФ
- 4 б. Закон "Об информации, информатизации и защите информации"
- 5 с. Конституция

10. Классификация и виды информационных ресурсов определены

- 1 а. Законом "Об информации, информатизации и защите информации"
- 2 б. Гражданским кодексом
- 3 с. Конституцией
- 4 d. всеми документами, перечисленными в остальных пунктах

Тема 3. Правовые режимы защиты конфиденциальной информации.

1. Формой правовой защиты литературных, художественных и научных произведений является (...) право

а. литературное

б. художественное

c. авторское

d. патентное

2. Запрещено относить к информации с ограниченным доступом

a. законодательные акты, информацию о чрезвычайных ситуациях и информацию ограниченного доступа

b. деятельности органов государственной власти (кроме государственной тайны)

a. только информацию о чрезвычайных ситуациях

b. только информацию о деятельности органов государственной власти (кроме

c. государственной тайны)

a. документы всех библиотек и архивов

3. Формой правовой защиты изобретений является

a. институт коммерческой тайны

b. патентное право

c. авторское право

d. все, перечисленное в остальных пунктах

4. К коммерческой тайне могут быть отнесены

a. сведения не являющиеся государственными секретами

b. сведения, связанные с производством и технологической информацией

c. сведения, связанные с управлением и финансами

d. сведения, перечисленные в остальных пунктах

5. Является ли авторское право, патентное право и КТ формами защиты интеллектуальной собственности?

a. да

b. нет

с. только авторское и патентное

d. только КТ

6. «Ноу-хау» это -

a. незащищенные новшества

b. защищенные новшества

с. общеизвестные новые технологии

d. опубликованные технические и технологические новинки

7. Каким законом в РФ защищаются права исполнителей и производителей фонограмм?

a. "О правовой охране программ для ЭВМ и баз данных"

b. "Об авторском праве и смежных правах"

с. "Патентный закон РФ"

d. закон еще не принят

8. Закон "Об авторском праве и смежных правах" защищает права

a. исполнителей (актеров, певцов и т.д.)

b. производителей фонограмм

с. организации эфирного и кабельного вещания

d. всех лиц, перечисленных в остальных пунктах

9. Какой законодательный акт содержит сведения по защите коммерческой тайны?

a. Закон "Об авторском праве и смежных правах"

b. Закон "О коммерческой тайне"

с. Патентный закон

d. Закон "О правовой охране программ для ЭВМ и баз данных"

10. К информации ограниченного доступа не относится

- a. государственная тайна
- b. размер золотого запаса страны
- c. персональные данные
- d. коммерческая тайна

11. Система защиты государственных секретов

- a. основывается на Уголовном Кодексе РФ
- b. регулируется секретными нормативными документами
- c. определена Законом РФ "О государственной тайне"
- d. осуществляется в соответствии с п. 1-3

12. Действие Закона "О государственной тайне" распространяется

- a. на всех граждан и должностных лиц РФ
- b. только на должностных лиц
- c. на граждан, которые взяли на себя обязательство выполнять требования
- b. законодательства о государственной тайне
- a. на всех граждан и должностных лиц, если им предоставили для работы закрытые
- c. сведения

13. К государственной тайне относится...

- a. информация в военной области
- b. информация о внешнеполитической и внешнеэкономической деятельности государства
- c. информация в области экономики, науки и техники и сведения в области разведывательной и оперативно-розыскной деятельности
- d. все выше перечисленное

14. Документы, содержащие государственную тайну снабжаются грифом

- a. "секретно"
- b. "совершенно секретно"
- c. "особой важности"
- d. указанным в п.1-3

15. Гриф "ДСП" используется

- a. для секретных документов
- b. для документов, содержащих коммерческую тайну
- c. как промежуточный для несекретных документов
- d. в учебных целях

16. Порядок засекречивания состоит в установлении следующих принципов:

- a. целесообразности и объективности
- b. необходимости и обязательности
- c. законности, обоснованности и своевременности
- d. всех выше перечисленных

17. Предельный срок пересмотра ранее установленных грифов секретности составляет

- a. 5 лет
- b. 1 год
- c. 10 лет
- d. 15 лет

18. Срок засекречивания сведений, составляющих государственную тайну

- a. составляет 10 лет

б. ограничен 30 годами

с. не ограничен

Тема 4. Лицензирование и сертификация в информационной сфере.

1. Лицензированием в области защиты информации называется:

а. деятельность, заключающаяся в передаче или получении прав на проведение работ в области защиты информации.

б. деятельность, заключающаяся в обработке или хранении документов

с. защита информации

2. Лицензией называется:

а. информация о внешнеполитической и внешнеэкономической деятельности государства

б. разрешение на право проведения работ в области защиты информации.

с. все выше перечисленное

3. На какой срок выдается лицензия?:

а. 5 лет

б. 1 год

с. 3 года

4. Что нужно делать после истечения срока действия лицензии?:

а. перерегистрация в порядке, установленном для выдачи лицензии

б. купить пробную версию лицензии

с. продолжать пользоваться продуктом без лицензии

5. Какие условия нужны для предприятия чтобы получить лицензию:

а. производственную и испытательную базу

б. нормативную и методическую документацию

с. располагает научным и инженерно-техническим персоналом

d. все выше перечисленное

6. Организационную структуру лицензирования образуют (два варианта ответа):

a. государственные органы по лицензированию

b. лицензионные центры

c. лицензируемые объекты

7. Государственные органы по лицензированию:

a. организуют обязательное государственное лицензирование деятельности предприятий

b. планируют и проводят работы по экспертизе предприятий-заявителей;

c. контролируют полноту и качество выполненных лицензиатами работ.

8. Лицензионные центры:

a. выдают государственные лицензии предприятиям-заявителям;

b. согласовывают составы экспертных комиссий, представляемые лицензионными центрами

c. формируют экспертные комиссии и представляют их состав на согласование руководителям соответствующих государственных органов по лицензированию, которыми являются ФСТЭК и ФСБ;

Тема 5. Компьютерные правонарушения.

1. Компьютерное преступление (два правильных ответа):

a. любое противоправное действие, при котором компьютер выступает либо как объект, против которого совершается преступление, либо как инструмент, используемый для совершения преступных действий.

b. хищение, шпионаж, незаконное собирание сведений, которые составляют коммерческую тайну, и т.д., если оно совершается с использованием компьютера

c. доступ к информации в нарушение должностных полномочий сотрудника, доступ к закрытой для публичного доступа информации со стороны лиц, не имеющих разрешения на доступ к этой информации.

2. Несанкционированный доступ:

- a. доступ к информации в нарушение должностных полномочий сотрудника, доступ к закрытой для публичного доступа информации со стороны лиц, не имеющих разрешения на доступ к этой информации.
- b. преступления, при совершении которых компьютерная техника, информация или электронная обработка информации выступают в качестве предмета или средства совершения преступления
- c. хищение, шпионаж, незаконное собирание сведений, которые составляют коммерческую тайну, и т.д., если оно совершается с использованием компьютера

3. Причины возникновения компьютерных преступлений:

- a. изменение идеологии хранения, обработки и передачи информации;
- b. использование программных средств, имеющих ошибки в кодах приложений;
- c. использование программных продуктов, не включающих системы защиты информации;
- d. все выше перечисленное

4. Неправомерный доступ к охраняемой законом компьютерной информации несет за собой денежный штраф в размере:

- a. до 500 т.р
- b. до 100 т.р
- c. до 200 т.р

5. Использование вредоносных компьютерных программ предназначены:

- a. для несанкционированного уничтожения
- b. блокирования
- c. модификации
- d. все выше перечисленное

6. типы вредоносных программ:

- a. вирусы, черви, троянские и хакерские программы
- b. шпионское, рекламное программное обеспечение, Вирусы
- c. потенциально опасное программное обеспечение, программы скрытого дозвона

7. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации наказывается штрафом в размере:

- a. до 500 т.р
- b. до 100 т.р
- c. до 200 т.р

8. Расположите вирусы по вредоносной нагрузке:

- a. Похищение данных, представляющих ценность или тайну.
- b. Саботирование промышленных процессов, управляемых компьютером (этим известен червь Stuxnet).
- c. Распаковка другой вредоносной программы, уже содержащейся внутри файла (dropper).
- d. Блокировка антивирусных сайтов, антивирусного ПО и административных функций ОС с целью усложнить лечение.

Тема 6. Внутренние нормативные документы по ИБ.

1. В число граней, позволяющих структурировать средства достижения информационной безопасности, входят:

- a. меры обеспечения целостности;
- b. административные меры;
- c. меры обеспечения конфиденциальности.

2. Дублирование сообщений является угрозой:

- a. доступности;
- b. конфиденциальности;
- c. целостности.

3. Вредоносное ПО Melissa подвергает атаке на доступность:

- a. системы электронной коммерции;
- b. геоинформационные системы;

с. системы электронной почты.

4. Выберите вредоносную программу, которая открыла новый этап в развитии данной области.

а. Melissa.

б. Bubble Boy.

с. ILO VE YOU.

5. Самыми опасными источниками внутренних угроз являются:

а. некомпетентные руководители;

б. обиженные сотрудники;

с. любопытные администраторы.

6. Среди нижеперечисленных выделите главную причину существования многочисленных угроз информационной безопасности.

а. просчеты при администрировании информационных систем;

б. необходимость постоянной модификации информационных систем;

с. сложность современных информационных систем.

7. Агрессивное потребление ресурсов является угрозой:

а. доступности

б. конфиденциальности

с. целостности

8. Программа Melissa — это:

а. бомба;

б. вирус;

с. червь.

9. Для внедрения бомб чаще всего используются ошибки типа:

- a. отсутствие проверок кодов возврата;
- b. переполнение буфера;
- c. нарушение целостности транзакций.

10. Окно опасности появляется, когда:

- a. становится известно о средствах использования уязвимости;
- b. появляется возможность использовать уязвимость;
- c. устанавливается новое ПО.

Тема 7. Угрозы. Система управления информационной безопасностью предприятия.

1. Криптография необходима для реализации следующих сервисов безопасности:

- a. идентификация;
- b. экранирование;
- c. аутентификация.

2. Криптография необходима для реализации следующих сервисов безопасности:

- a. контроль конфиденциальности;
- b. контроль целостности;
- c. контроль доступа.

3. Экран выполняет функции:

- a. разграничения доступа;
- b. облегчения доступа;
- c. усложнения доступа.

4. Демилитаризованная зона располагается:

- a. перед внешним межсетевым экраном;

b. между межсетевыми экранами;

c. за внутренним межсетевым экраном.

5. Экранирование на сетевом и транспортном уровнях может обеспечить:

a. разграничение доступа по сетевым адресам;

b. выборочное выполнение команд прикладного протокола;

c. контроль объема данных, переданных по ТСП-соединению.

6. Системы анализа защищенности помогают предотвратить:

a. известные атаки;

b. новые виды атак;

c. нетипичное поведение пользователей.

7. Среднее время наработки на отказ:

a. пропорционально интенсивности отказов;

b. обратно пропорционально интенсивности отказов;

c. не зависит от интенсивности отказов.

8. Туннелирование может использоваться на следующем уровне эталонной семиуровневой модели OSI:

a. сетевом;

b. сеансовом;

c. уровне представления.

9. Принцип усиления самого слабого звена можно переформулировать как:

a. принцип равной прочности обороны;

b. принцип удаления слабого звена;

с. принцип выявления главного звена, ухватившись за которое, можно вытянуть всю цепь.

10. Политика безопасности:

- a. фиксирует правила разграничения доступа;
- b. отражает подход организации к защите своих информационных активов;
- с. описывает способы защиты руководства организации.

11. При анализе стоимости защитных мер следует учитывать:

- a. расходы на закупку оборудования
- b. расходы на закупку программ
- с. расходы на обучение персонала

Тема 8. Математическое моделирование, программная реализация и анализ протоколов безопасной передачи данных как динамических систем.

1. Виды компьютерно-технической экспертизы:

- a. Аппаратно-компьютерная экспертиза;
- b. Программно-компьютерная экспертиза
- с. Компьютерно-сетевая экспертиза;
- d. все вышеперечисленные

2. Обычно перед экспертом ставятся вопросы:

- a. о возможности (пригодности) использования исследуемых объектов для определённых целей (например, для доступа в сеть);
- b. о стоимости компьютеров, носителей, лицензий на содержащиеся там программы;
- с. о переводах найденных текстов, интерфейсов программ, переписки и т. п.

3. Следующие вопросы не должны относиться к данному виду экспертизы, их включение в постановление представляется ошибочным:

- a. о свойствах программ для ЭВМ, в частности, о принадлежности их к вредоносным;

б. об идентификации найденных электронных документов, программ для ЭВМ, пользователей компьютера.

с. о лицензионности/контрафактности экземпляров программ, записанных на исследуемых объектах;

4.Используемые программы:

а. DeFacto

б. CCleaner

с. Booster

5.Класс аппаратных объектов:

а. компьютеры персональные (ноутбуки, настольные, портативные);

б. стол

с. шкаф

6.Вопросы для компьютерно-технической экспертизы аппаратных средств(два ответа):

а. определить, относится ли представленное устройство к аппаратным компьютерным средствам;

б. определить совместимость конкретного программного средства с программным и аппаратным обеспечением компьютерной системы;

с. определить, используется ли данное программное средство для решения определенной функциональной задачи;

д. определить, к какому типу (марке, модели)относится аппаратное (компьютерное) средство;

7.Вопросы компьютерно-технической экспертизе программных средств(два ответа):

а. определить, какую классификацию имеют конкретные программные средства (системные или прикладные) представленного программного обеспечения;

б. определить общую характеристика представленного на судебную компьютерно-техническую экспертизу программного обеспечения, из каких компонент (программных средств) оно состоит;

с. определить, какое запоминающее устройство предназначено для работы с данным накопителем информации;

д. определить, имеется ли в составе представленного компьютера, какое-либо запоминающее устройство для работы с этим носителем информации;

8. Вопросы компьютерно-технической экспертизе информации (данных) (два ответа):

- a. определить, имеются ли в программном средстве отклонения от нормальных параметров (например, свойства инфицирования, недокументированных функций);
- b. определить характеристики физического размещения данных на носителе информации (компьютере);
- c. определить, каким образом организованы ввод и вывод данных в представленном компьютере (программном средстве);
- d. определить, каким образом был отформатирован носитель информации (компьютер) и в каком виде на него записаны данные;

Тема 9. Организация технической защиты информации.

1. В соответствии с терминологией Закона №149 ФЗ «Об информации, информационных технологиях и защите информации» информация это

- a. сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления
- b. защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.
- c. характерное свойство объекта защиты, которое может быть использовано технической разведкой для обнаружения и распознавания объекта, а также для получения необходимых сведений о нем.

2. Защите не подлежит информация:

- a. секретная
- b. конфиденциальная
- c. своевременная

3. Дайте определение Государственной тайны:

- a. сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления
- b. защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

с. характерное свойство объекта защиты, которое может быть использовано технической разведкой для обнаружения и распознавания объекта, а также для получения необходимых сведений о нем.

4. Под конфиденциальной понимается информация с:

- а. ограниченным доступом, не содержащая государственную тайну
- б. неограниченным доступом
- с. с ограниченным доступом, содержащая государственную тайну

5. Под демаскирующим признаком понимается свойство объекта:

- а. связанное с функционированием объекта защиты и проявляющееся через их физические поля
- б. которое может быть использовано технической разведкой для обнаружения и распознавания объекта
- с. отличаться по каким-либо характеристикам от других объектов.

6. Что не относится к основным источникам функциональных сигналов относятся:

- а. источники систем связи
- б. передатчики радиотехнических систем
- с. распространители электромагнитных сигналов

7. Обнаружение объекта это

- а. процесс функционирования средства технической разведки (ТР), в результате которого фиксируются технические демаскирующие признаки объекта и делается заключение о его наличии.
- б. процесс функционирования средства ТР, в результате которого определяются параметры демаскирующего признака объекта и делается заключение о его характеристиках
- с. техническое средство, предназначенное для устранения или ослабления демаскирующих признаков объекта, создания ложных (имитирующих) признаков, а также для создания помех техническим средствам доступа к информации

8. Что такое семантическая информация:

- а. процесс функционирования средства технической разведки

- b. продукт абстрактного мышления человека и обработки данных рецепторов других живых существ
- c. сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления

Тема 10. Интеллектуальная собственность и ее защита.

1. Что представляет собой ресурс системы защиты информации?

- a. количество специалистов по защите информации
- b. состав инженерно-технических сооружений
- c. выделенные денежные средства
- d. все выше перечисленное

2. Что надо определить перед выбором мер защиты информации?

- a. квалификацию персонала
- b. угрозы безопасности информации
- c. систему пожарно-охранной сигнализации

3. Локальные показатели эффективности защиты информации подразделяются на:

- a. тактические и стратегические
- b. оперативные и постоянные
- c. функциональные и экономические
- d. территориальные и пространственные

4. Что означает принцип экономичности защиты информации?

- a. минимизация затрат на защиту информации
- b. затраты на защиту информации не должны превышать возможный ущерб от реализации угроз
- c. численность службы защиты информации не должна превышать 7 чел.
- d. комплексное использование различных способов и средств защиты информации

5. Что означает принцип рациональности защиты информации?

- a. использование только сертифицированных средств защиты
- b. системный подход к инженерно—технической защите информации
- c. минимизацию ресурсов на обеспечение необходимого уровня безопасности информации
- d. все вместе

6. Зоны защиты объектов информатизации бывают:

- a. независимыми, пересекающимися и вложенными
- b. автономными, многоярусными и многозвенными
- c. укрепленными, локальными и общими

7. Чем отличаются ОТСС от ВТСС?

- a. потребляемой мощностью
- b. наличием принятых мер по защите информации
- c. не могут использоваться для обработки открытой информации
- d. большей скоростью обработки информации

8. По способу формирования электрического сигнала активные акустоэлектрические преобразователи могут быть

- a. индуктивными, электродинамическими и пьезоэлектрическими
- b. емкостными, электродинамическими и электромагнитными
- c. электродинамическими, электромагнитными и пьезоэлектрическими
- d. индуктивными, емкостными и резистивными

9. Чувствительность электродинамического микрофона лежит в пределах

- a. 30 - 45 мВ/Па
- b. 4 - 6 мВ/Па
- c. 0,1 – 0,5 мВ/Па

d. 0,001 – 0,2 мВ/Па

10. Чувствительность вторичных электрических часов как акустоэлектрических преобразователей

a. 30 - 45 мВ/Па

b. 4 - 6 мВ/Па

c. 0,1 – 0,5 мВ/Па

d. 0,001 – 0,2 мВ/Па

Тема 11. Информационно-аналитическое обеспечение правоохранительной деятельности.

1. К объектам интеллектуальной собственности относятся:

a. селекционные достижения;

b. товары и услуги;

c. произведения прикладного искусства;

d. секреты производства (ноу-хау);

e. фонограммы;

f. логотипы;

g. музыкальные произведения.

2. Правовая охрана каких объектов интеллектуальной собственности возникает в силу факта их создания:

a. литературных произведений;

b. изобретений;

c. компьютерных программ;

d. фотографий;

e. промышленных образцов.

3. Результат интеллектуальной деятельности может одновременно использоваться:

одним лицом;

- a. группой лиц до 10 человек;
- b. группой лиц более 10 человек;
- c. неограниченным кругом лиц.

4. К объектам авторского права относятся:

- a. новые сорта растений;
- b. музыкальные произведения;
- c. товарные знаки;
- d. идеи, концепции, открытия;
- e. научные статьи.

5. Авторское право возникает:

- a. с момента возникновения идеи произведения;
- b. после регистрации произведения и получения свидетельства;
- c. с момента создания произведения.

6. Какой из объектов охраняется правом интеллектуальной собственности:

- a. недвижимое имущество;
- b. идея;
- c. герб;
- d. товарный знак;
- e. открытие.

7. Выберите объект, правовая охрана которого удостоверяется патентом:

- a. картина;
- b. песня;

- c. изобретение;
- d. товар;
- e. курсовая работа.

8. Для правовой охраны каких объектов не требуется получение патента:

- a. картина;
- b. изобретение;
- c. промышленный образец;
- d. произведение архитектуры;
- e. дипломная работа.

Тема 12. Информационно-психологическое обеспечение правоохранительной деятельности.

1. Сущность информационного обеспечения правоохранительных органов определяется как:

- a. целесообразная деятельность человека, направленная на исходные фактические данные с тем, чтобы, используя соответствующие технические средства, преобразовать их в форму, пригодную для решения управленческих либо конкретных задач выявления, предупреждения, пресечения и раскрытия правонарушений и преступлений, розыска скрывшихся правонарушителей и преступников, а также без вести пропавших граждан.
- b. системность информации, а также непрерывность ее сбора и анализа.
- c. механизм управления правоохранительными органами

2. Одним из основных требований, предъявляемых к организации информационно-аналитического обеспечения правоохранительных органов, является:

- a. автономность системы
- b. системность информации, а также непрерывность ее сбора и анализа.
- c. решение управленческих либо конкретных задач

3. Основным объектом информационной деятельности правоохранительных органов является:

- a. интеллектуальная обработка информации
- b. информационно-аналитическая работа

с. информация социального характера

4. Информационно-аналитическая деятельность является целостной частью:

а. ведомственного механизма управления правоохранительными органами

б. управленческой деятельности

с. системы включающей в себя два взаимосвязанных компонента

5. Важной процедурой информационно-аналитическая работа является:

а. оптимизации информационного обеспечения деятельности правоохранительных органов

б. интеллектуальная обработка информации

с. первичный анализ и отбор релевантной информации

6. Информационное обеспечение правоохранительных органов ориентировано прежде всего на:

а. интеллектуальную обработку информации

б. поддержание устойчивого состояния информационных связей

с. сборе, накоплении, обработке, хранении и выдаче информации потребителям в максимально короткие сроки

7. Информационное обеспечение административной деятельности органов внутренних дел включает в себя:

а. правовую информацию

б. массив различных неправовых источников информации

с. все вышеперечисленное

8. В целях защиты интересов Российской Федерации и граждан от преступных посягательств, действуя в рамках своей компетенции, органы внутренних дел используют возможности:

а. информационного обеспечения в процессе розыска и идентификации лиц, выявления, предупреждения, пресечения и раскрытия преступлений по находящимся в их производстве материалам и уголовным делам

б. систематизации и анализа информации

с. выявление детерминант того или иного явления

9. Роль прокуратуры в системе правоохранительных органов и возложение на нее функций общего надзора за соблюдением законодательства в России обуславливает:

- а. необходимость учета в организации информационно-аналитического обеспечения ее деятельности огромного объема самой разнообразной информации
- б. получения информации должностными лицами прокуратуры
- с. информационным взаимодействием с органами государственной власти

Тема 13. Организационная защита информации.

1. Психологическое обеспечение в сфере правоохранения имеет одну из форм осуществления:

- а. консультационная помощь специалиста-психолога
- б. конкретные меры психологического характера, направленные на достижение определенной цели
- с. потребности системы, цели и задачи, соответствующие требованию повышения эффективности работы

2. К консультационной помощи специалиста прибегают в том случае, когда

- а. показания специалиста – сообщение сведений о фактах, известных ему как лицу
- б. правоохранительным органам могут потребоваться специальные знания, умения и навыки
- с. критический анализ заключения психолога в форме документа «мнение специалиста»

3. Консультационная помощь не включает в себя:

- а. консультации в форме допроса специалиста по иным вопросам, входящим в его компетенцию, осуществляемые сведущим лицом;
- б. критический анализ заключения психолога в форме документа «мнение специалиста»;
- с. конкретные меры психологического характера, направленные на достижение определенной цели

4. К экспертным учреждениям не относят:

- а. судебно-психологические институты
- б. комплексные экспертизы институты

с. суд

5. Во главе системы экспертных учреждений в структуре Министерства юстиции стоит:

- а. Российский Федеральный центр судебных экспертиз
- б. Министерства здравоохранения и медицинской промышленности
- с. Государственный центр социальной и судебной психиатрии им. В.П. Сербского

6. Право производства комплексных судебных психолого-психиатрических экспертиз принадлежит экспертным учреждениям

- а. Российский Федеральный центр судебных экспертиз
- б. Министерства здравоохранения и медицинской промышленности
- с. Государственный центр социальной и судебной психиатрии им. В.П. Сербского

7. Где расположена сеть экспертных учреждений в Вооруженных Силах России:

- а. не существует
- б. только в крупных городах
- с. в округах, на флотах, в некоторых войсковых соединениях

8. Психолог, работающий в рамках экспертного учреждения, имеет особый:

- а. отличительный знак
- б. процессуальный статус эксперта
- с. документ

9. Под психологической службой понимают

- а. комплексное использование данных психологической науки, ее средств, методов и технологий специально подготовленными или компетентными в этой сфере лицами в целях совершенствования деятельности органов правоохранения

в. возможность в соответствии с целями и направлениями обеспечения выделить направления, цели и задачи деятельности юридического психолога по осуществлению психологического обеспечения правоохранительной деятельности, которые составляют программу его профессиональной деятельности

с. централизованно управляемую систему специальных структурных подразделений и должностей специалистов

10. В уголовно-исполнительной системе активное создание психологической службы обусловлено

а. историческим опытом использования психологических знаний в данном ведомстве

б. ростом преступности

с. экономическим развитием

4.3 Промежуточная аттестация по дисциплине проводится в форме зачета, экзамена

Типовые вопросы зачета (ПК-3)

Типовые задания для зачета (ПК-3)

Типовые вопросы экзамена (ПК-3)

1. Понятие информации. Документированная информация
2. Доктрина информационной безопасности Российской Федерации. Стратегия национальной безопасности Российской Федерации до 2020 года.
3. Конфиденциальная информация: понятие, признаки, классификация.
4. Понятия лицензирования и сертификации.
5. Понятие компьютерных преступлений. Неправомерный доступ к компьютерной информации
6. Политика ИБ. Обязательство о неразглашении защищаемых сведений.
7. Основные функции систем управления информационной безопасностью. Принципы управления информационной безопасностью
8. Виды информации, защищаемой техническими средствами. Свойства информации, влияющие на возможности ее защиты
9. Краткая характеристика государственной системы защиты информации.
10. Организационные и технические меры по инженерно-технической защите информации в организации
11. Интеллектуальный продукт как объект интеллектуальной собственности и предмет защиты.
12. Авторское право. Патентное право. Товарный знак
13. Методика информационно-аналитической работы. Основа работы с информацией.
14. Психологические аспекты формирования профессиональных качеств сотрудника
15. Психологическая подготовка сотрудников органов внутренних дел.
16. Организация службы безопасности объекта.
17. Судебная власть: понятие и основные признаки
18. Основные суды, суды среднего звена и высшие суды. Понятие судебной инстанции.
19. Понятие уязвимости. Классификация угроз.

Типовые задания для экзамена (ПК-3)

1. Организационные меры и основные правила работы за компьютером.

2. Определение надёжности персональных межсетевых экранов.
3. Базовые способы и возможности защиты программного обеспечения с помощью электронных ключей.
4. Понятие о проверке электронной подписи .
5. Преимущества и недостатки систем с симметричными ключами.
6. Понятие блочного шифра.

4.4. Шкала оценивания промежуточной аттестации

Зачет

Оценка	Компетенции	Дескрипторы (уровни) – основные признаки освоения (показатели достижения результата)
«зачтено» (50 - 100 баллов)	ПК-3	Демонстрирует высокий уровень теоретических знаний о методах расследования компьютерных инцидентов. Способен выявлять признаки несанкционированного доступа, определять место и время совершения преступления. Умеет организовывать работы по расследованию компьютерных инцидентов как часть технологического процесса защиты информации в компьютерных системах.
«не зачтено» (0 - 49 баллов)	ПК-3	Не способен продемонстрировать знания о методах расследования компьютерных инцидентов. Не способен выявлять признаки несанкционированного доступа, определять место и время совершения преступления. Не умеет организовывать работы по расследованию компьютерных инцидентов как часть технологического процесса защиты информации в компьютерных системах.

Экзамен

Оценка	Компетенции	Дескрипторы (уровни) – основные признаки освоения (показатели достижения результата)
«отлично» (85 - 100 баллов)	ПК-3	Демонстрирует высокий уровень теоретических знаний в области обеспечения защиты информации в критически важной информационной инфраструктуре. Понимает современные подходы и технологии обеспечения информационной безопасности. Способен проводить работы по администрированию средств защиты информации прикладного и системного программного обеспечения.
«хорошо» (70 - 84 баллов)	ПК-3	Демонстрирует хороший уровень теоретических знаний в области обеспечения защиты информации в критически важной информационной инфраструктуре. Достаточно хорошо понимает современные подходы и технологии обеспечения информационной безопасности. Способен проводить работы по администрированию средств защиты информации прикладного и системного программного обеспечения.

«удовлетворительно» (50 - 69 баллов)	ПК-3	Демонстрирует низкий уровень теоретических знаний в области обеспечения защиты информации в критически важной информационной инфраструктуре. Слабо понимает современные подходы и технологии обеспечения информационной безопасности. Затрудняется с проведением работы по администрированию средств защиты информации прикладного и системного программного обеспечения.
«неудовлетворительно» (менее 50 баллов)	ПК-3	Не способен продемонстрировать знания в области обеспечения защиты информации в критически важной информационной инфраструктуре. Не понимает современные подходы и технологии обеспечения информационной безопасности. Не способен проводить работы по администрированию средств защиты информации прикладного и системного программного обеспечения.

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. Лопатин Д.В., Калинина Ю.В. Безопасные информационные технологии : электрон. учеб. пособие. - Тамбов: [Б.и.], 2014. - 1 электрон. опт. диск (CD-ROM)
2. Тамб гос. ун-т им. Г.Р. Державина, Ин-т математики, физики и информатики Техническая защита информации : учеб. пособие. - Тамбов: [Б.и.], 2014. - 1 электрон. опт. диск (CD-ROM)

6.2 Дополнительная литература:

1. Загинайлов Ю. Н. Основы информационной безопасности: курс визуальных лекций : учебное пособие. - Москва|Берлин: Директ-Медиа, 2015. - 105 с. - Текст : электронный // ЭБС «Университетская библиотека онлайн» [сайт]. - URL: <http://biblioclub.ru/index.php?page=book&id=362895>
2. Загинайлов Ю. Н. Теория информационной безопасности и методология защиты информации : учебное пособие. - Москва|Берлин: Директ-Медиа, 2015. - 253 с. - Текст : электронный // ЭБС «Университетская библиотека онлайн» [сайт]. - URL: <http://biblioclub.ru/index.php?page=book&id=276557>
3. Аверченков В. И., Рытов М. Ю., Кувыклин А. В., Рудановский М. В. Аудит информационной безопасности органов исполнительной власти : учебное пособие. - 4-е изд., стер.. - Москва: Флинта, 2016. - 100 с. - Текст : электронный // ЭБС «Университетская библиотека онлайн» [сайт]. - URL: <http://biblioclub.ru/index.php?page=book&id=93259>

6.3 Иные источники:

1. Курс «Стандарты информационной безопасности» - <https://www.intuit.ru/studies/courses/30/30/info>
2. Курс «Основы информационной безопасности» - <https://www.intuit.ru/studies/courses/10/10/info>

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 и свободно распространяемое программное обеспечение:

Microsoft Office Профессиональный плюс 2007

Профессиональные базы данных и информационные справочные системы:

1. Электронная библиотека РФФИ. – URL: <https://www.rfbr.ru/rffi/ru/library>
2. Российская национальная библиотека: официальный сайт. – URL: <http://nlr.ru>
3. Российская государственная библиотека: официальный сайт. – URL: <https://www.rsl.ru>
4. Научная электронная библиотека eLIBRARY.ru. – URL: <https://elibrary.ru>
5. Консультант студента. Гуманитарные науки: электронно-библиотечная система. – URL: <https://www.studentlibrary.ru>
6. Университетская библиотека онлайн: электронно-библиотечная система. – URL: <https://biblioclub.ru>

7. Электронный каталог Фундаментальной библиотеки ТГУ. – URL: <https://www.tsutmb.ru/biblio/elektronnyij-katalog/>
8. Президентская библиотека имени Б.Н. Ельцина. – URL: <https://www.prlib.ru>
9. Научная электронная библиотека Российской академии естествознания. – URL: <https://www.monographies.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.