

Программу составил(и):

старший преподаватель, Алферова В.В.

Рецензент(ы):

д.т.н., Профессор кафедры информатики и вычислительной техники КубГТУ, Хисамов Ф.Г.; директор АО «ЮГ-СИСТЕМА ПЛЮС», Глебов О.В.

Рабочая программа дисциплины

Порядок проведения аттестации объектов информатизации

разработана в соответствии с ФГОС ВО:

Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 10.03.01 Информационная безопасность (приказ Минобрнауки России от 17.11.2020 г. № 1427)

составлена на основании учебного плана:

10.03.01 Информационная безопасность

утвержденного учёным советом вуза от 20.11.2023 протокол № 3.

Рабочая программа одобрена на заседании кафедры

Кафедра математики и вычислительной техники

Протокол от 13.10.2023 г. № 3

Зав. кафедрой Исикова Наталья Павловна

Согласовано с представителями работодателей на заседании НМС, протокол № 3 от 20.11.2023.

Председатель НМС проф. Павелко Н.Н.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	формирование у студентов системных знаний по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну, а также требованиям к процессам, форме и содержанию документов, разрабатываемых при проведении этих работ
<p>Задачи: 1.Формирование системных знаний о порядке аттестации объектов информатизации на соответствие требованиям по защите информации;</p> <p>Изучение нормативно-правовых актов по обеспечению процедуры аттестации объектов информатизации на соответствие требованиям о защите информации.;</p> <p>Освоение необходимых знаний для организации мероприятий по аттестации объектов информатизации, а так же состава работ по проведению аттестационных испытаний:</p> <p>Формирование умений и навыков по формированию и реализации программы и методики аттестационных испытаний объекта информатизации;</p>	

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.В
2.1	Требования к предварительной подготовке обучающегося:
2.1.1	Информатика
2.1.2	Введение в направление подготовки и планирование профессиональной карьеры
2.2	Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:
2.2.1	Выполнение и защита выпускной квалификационной работы
2.2.2	Производственная практика: Преддипломная практика

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ, ИНДИКАТОРЫ ИХ ДОСТИЖЕНИЯ и планируемые результаты обучения	
ПК-6: Способен документально оформлять работы по обеспечению информационной безопасности	
ПК-6.1: Анализирует полноту и нормативным требованиям руководящих документов, описывающих работы по обеспечению информационной безопасности	
Знать	
Уровень 1	Минимальный необходимый уровень знаний анализа полноты и нормативных требований руководящих документов, описывающих работы по обеспечению информационной безопасности
Уровень 2	Уровень знаний анализа полноты и нормативных требований руководящих документов, описывающих работы по обеспечению информационной безопасности в объёме, соответствующем программе подготовки, допущено несколько негрубых ошибок
Уровень 3	Уровень знаний анализа полноты и нормативных требований руководящих документов, описывающих работы по обеспечению информационной безопасности в объёме, соответствующем программе подготовки, без ошибок
ПК-6.2: Формирует отчётные и руководящие документы для обеспечения защиты информации в информационной системе в ходе ее эксплуатации	
Уметь	
Уровень 1	Продемонстрированы основные умения формировать отчётные и руководящие документы для обеспечения защиты информации в информационной системе в ходе ее эксплуатации, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения формировать отчётные и руководящие документы для обеспечения защиты информации в информационной системе в ходе ее эксплуатации, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы все основные умения формировать отчётные и руководящие документы для обеспечения защиты информации в информационной системе в ходе ее эксплуатации, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме
ПК-6.3: Формулирует в соответствии с требованиям руководящих документов состав и содержание процедур контроля обеспеченности уровня защищенности информации	
Владеть	
Уровень 1	Имеется минимальный набор навыков формулировать в соответствии с требованиям руководящих документов состав и содержание процедур контроля обеспеченности уровня защищенности информации с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки формулировать в соответствии с требованиям руководящих документов состав и содержание процедур контроля обеспеченности уровня защищенности информации с некоторыми недочётами
Уровень 3	Продемонстрированы навыки формулировать в соответствии с требованиям руководящих документов состав и содержание процедур контроля обеспеченности уровня защищенности информации без ошибок и недочётов

ПК-6.4: Готовит документы для проведения работ по аттестации объектов информатизации и автоматизированных систем	
Уметь	
Уровень 1	Продемонстрированы основные умения готовить документы для проведения работ по аттестации объектов информатизации и автоматизированных систем, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения готовить документы для проведения работ по аттестации объектов информатизации и автоматизированных систем, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы все основные умения готовить документы для проведения работ по аттестации объектов информатизации и автоматизированных систем, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетенции	Литература и эл. ресурсы	Практ. подг.
	Раздел 1. Раздел 1.					
1.1	Основные понятия в области технической защиты информации /Лек/	8	4	ПК-6.1 ПК-6.2 ПК-6.3 ПК-6.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.2	Основные понятия в области технической защиты информации /Пр/	8	4	ПК-6.1 ПК-6.2 ПК-6.3 ПК-6.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.3	Основные понятия в области технической защиты информации /Ср/	8	8,8	ПК-6.1 ПК-6.2 ПК-6.3 ПК-6.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.4	Концептуальные основы защиты информации. Система документов по технической защите информации. /Лек/	8	2	ПК-6.1 ПК-6.2 ПК-6.3 ПК-6.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.5	Концептуальные основы защиты информации. Система документов по технической защите информации. /Пр/	8	2	ПК-6.1 ПК-6.2 ПК-6.3 ПК-6.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.6	Концептуальные основы защиты информации. Система документов по технической защите информации. /Ср/	8	8,8	ПК-6.1 ПК-6.2 ПК-6.3 ПК-6.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.7	Органы по технической защите информации в РФ. /Лек/	8	2	ПК-6.1 ПК-6.2 ПК-6.3 ПК-6.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.8	Органы по технической защите информации в РФ. /Пр/	8	2	ПК-6.1 ПК-6.2 ПК-6.3 ПК-6.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.9	Органы по технической защите информации в РФ. /Ср/	8	8,8	ПК-6.1 ПК-6.2 ПК-6.3 ПК-6.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.10	Лицензирование деятельности в области ТЗИ. /Лек/	8	4	ПК-6.1 ПК-6.2 ПК-6.3 ПК-6.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.11	Лицензирование деятельности в области ТЗИ. /Пр/	8	4	ПК-6.1 ПК-6.2 ПК-6.3 ПК-6.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.12	Лицензирование деятельности в области ТЗИ. /Ср/	8	8,8	ПК-6.1 ПК-6.2 ПК-6.3 ПК-6.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.13	Объект информатизации. Классификация объектов защиты. /Лек/	8	4	ПК-6.1 ПК-6.2 ПК-6.3 ПК-6.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	

1.14	Объект информатизации. Классификация объектов защиты. /Пр/	8	4	ПК-6.1 ПК-6.2 ПК-6.3 ПК-6.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.15	Объект информатизации. Классификация объектов защиты. /Ср/	8	8,8	ПК-6.1 ПК-6.2 ПК-6.3 ПК-6.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.16	Общий порядок сертификации средств защиты информации /Лек/	8	4	ПК-6.1 ПК-6.2 ПК-6.3 ПК-6.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.17	Общий порядок сертификации средств защиты информации /Пр/	8	4	ПК-6.1 ПК-6.2 ПК-6.3 ПК-6.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.18	Общий порядок сертификации средств защиты информации /Ср/	8	8,8	ПК-6.1 ПК-6.2 ПК-6.3 ПК-6.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.19	Порядок сертификации во ФСТЭК России /Лек/	8	4	ПК-6.1 ПК-6.2 ПК-6.3 ПК-6.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.20	Порядок сертификации во ФСТЭК России /Пр/	8	4	ПК-6.1 ПК-6.2 ПК-6.3 ПК-6.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.21	Порядок сертификации во ФСТЭК России /Ср/	8	8,8	ПК-6.1 ПК-6.2 ПК-6.3 ПК-6.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.22	Аттестация объекта информатизации по требованиям безопасности информации /Лек/	8	4	ПК-6.1 ПК-6.2 ПК-6.3 ПК-6.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.23	Аттестация объекта информатизации по требованиям безопасности информации /Пр/	8	4	ПК-6.1 ПК-6.2 ПК-6.3 ПК-6.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.24	Аттестация объекта информатизации по требованиям безопасности информации /Ср/	8	8,8	ПК-6.1 ПК-6.2 ПК-6.3 ПК-6.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.25	Требования и рекомендации по защите информации, обрабатываемой средствами вычислительной техники /Лек/	8	4	ПК-6.1 ПК-6.2 ПК-6.3 ПК-6.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.26	Требования и рекомендации по защите информации, обрабатываемой средствами вычислительной техники /Пр/	8	4	ПК-6.1 ПК-6.2 ПК-6.3 ПК-6.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.27	Требования и рекомендации по защите информации, обрабатываемой средствами вычислительной техники /Ср/	8	9,4	ПК-6.1 ПК-6.2 ПК-6.3 ПК-6.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
	Раздел 2. Промежуточная аттестация					
2.1	Зачет /КА/	8	0,2	ПК-6.1 ПК-6.2 ПК-6.3 ПК-6.4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

5.1. Контрольные вопросы и задания

1. Что представляет собой объект информатизации?
2. Какие основные требования безопасности должны быть выполнены объектом информатизации?
3. Каковы этапы планирования аттестации объекта информатизации?
4. Что такое процедура обзора объекта информатизации?
5. Какие требования необходимо определить перед проведением аттестации?

6. Какие методы проверки могут быть использованы в процессе аттестации?
7. Что включает оценка результатов аттестации объекта информатизации?
8. Какой отчет должен быть подготовлен после проведения аттестации объекта информатизации?
9. Какие рекомендации могут быть содержаться в отчете после аттестации?
10. Какое решение может быть принято на основе результатов аттестации объекта информатизации?
11. Что должно быть документировано в результате аттестации объекта информатизации?
12. Какие меры могут быть приняты для устранения выявленных недостатков после аттестации?
13. Какие вопросы могут относиться к безопасности информационных систем при аттестации?
14. Какие вопросы могут относиться к системному администрированию при аттестации объектов информатизации?
15. Какие вопросы могут относиться к защите персональных данных при аттестации?
16. Что такое программирование в контексте аттестации объектов информатизации?
17. Какое значение имеет документирование результатов аттестации объектов информатизации?
18. Какие меры обеспечения безопасности могут быть предприняты перед проведением аттестации?
19. Каковы недостатки, которые могут быть обнаружены в результате аттестации объекта информатизации?
20. Какие преимущества имеет аттестация объектов информатизации с точки зрения безопасности и качества работы системы?

5.2. Темы письменных работ

1. Понятие и значение аттестации объектов информатизации.
2. Основные этапы планирования аттестации объектов информатизации.
3. Методы и процедуры обзора объектов информатизации в рамках аттестации.
4. Важность определения требований безопасности перед проведением аттестации.
5. Роль системного администрирования в процессе аттестации объектов информатизации.
6. Оценка результатов аттестации и принятие решений на их основе.
7. Подготовка и содержание отчета после аттестации объектов информатизации.
8. Вопросы, относящиеся к безопасности информационных систем при аттестации.
9. Вопросы, связанные с защитой персональных данных при аттестации.
10. Процесс программирования в контексте аттестации объектов информатизации.
11. Меры обеспечения безопасности перед проведением аттестации.
12. Недостатки, которые можно обнаружить в результате аттестации объектов информатизации.
13. Роль и значение документирования результатов аттестации объектов информатизации.
14. Преимущества аттестации объектов информатизации с точки зрения безопасности и качества работы системы.
15. Факторы, влияющие на успешность аттестации объектов информатизации.
16. Особенности проведения аттестации объектов информатизации в государственных структурах.
17. Значение подготовки сотрудников к аттестации объектов информатизации.
18. Меры, которые могут быть предприняты для устранения выявленных недостатков после аттестации.
19. Роль сертификации и аккредитации в процессе аттестации объектов информатизации.
20. Сравнение национальных и международных стандартов в области аттестации объектов информатизации.

5.3. Фонд оценочных средств

Из перечисленного базовыми услугами для обеспечения безопасности компьютерных систем и сетей являются

- 1) аутентификация;
- 2) идентификация;
- 3) целостность;
- 4) контроль доступа;
- 5) контроль трафика;
- 6) причастность.

Готовность устройства к использованию всякий раз, когда в этом возникает необходимость, характеризует свойство:

- 1) Целостность;
- 2) Доступность;
- 3) Детерминированность;
- 4) Восстанавливаемость.

Гарантия сохранности данными правильных значений, которая обеспечивается запретом для неавторизованных пользователей каким-либо образом модифицировать, разрушать или создавать данные - это

- 1) Доступность;
- 2) Детерминированность;
- 3) Целостность.
- 4) Восстанавливаемость

Информация - это

- 1) Только сведения, содержащиеся в электронных базах данных;
- 2) Только документированные сведения о лицах, предметах, фактах, событиях;
- 3) Сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.
- 4) Сведения, поступающие от СМИ

Защита информации это:

- 1) получение субъектом возможности ознакомления с информацией, в том

- числе при помощи технических средств;
- 2) процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
 - 3) деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.
 - 4) совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям
 - 5) преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа

Что такое политика безопасности?

- 1) Пошаговые инструкции по выполнению задач безопасности;
- 2) Детализированные документы по обработке инцидентов безопасности;
- 3) Общие руководящие требования по достижению определенного уровня безопасности.
- 4) Широкие, высокоуровневые заявления руководства

Информация

- 1) Становится доступной, если она содержится на материальном носителе;
- 2) Характеризуется всеми перечисленными свойствами;
- 3) Не исчезает при потреблении.
- 4) Подвергается только "моральному износу"

Перехват данных является угрозой

- 1) Целостности;
- 2) Доступности;
- 3) Конфиденциальности.

Естественные угрозы безопасности информации вызваны

- 1) Воздействиями объективных физических процессов или стихийных природных явлений, независимых от человека;
- 2) Ошибками при проектировании АСОИ, её элементов или разработке программного обеспечения;
- 3) Корыстными устремлениями злоумышленников.
- 4) Деятельностью человека
- 5) Ошибками при действиях персонала

Искусственные угрозы безопасности информации вызваны:

- 1) Ошибками при действиях персонала;
- 2) Корыстными устремлениями злоумышленников;
- 3) Ошибками при проектировании АСОИ, её элементов или разработке программного обеспечения.
- 4) Деятельностью человека
- 5) Воздействиями объективных физических процессов или стихийных природных явлений, независимых от человека

5.4. Перечень видов оценочных средств

Задания со свободно конструируемым ответом (СКО) предполагает составление развернутого ответа на теоретический вопрос. Задание с выбором одного варианта ответа (ОВ, в задании данного типа предлагается несколько вариантов ответа, среди которых один верный. Задания со свободно конструируемым ответом (СКО) предполагает составление развернутого ответа, включающего полное решение задачи с пояснениями.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год
Л1.1	Шаньгин В. Ф.	Информационная безопасность компьютерных систем и сетей	Москва: Форум, 2021, URL: https://ibooks.ru/reading.php?short=1&productid=361273
Л1.2	Медведев В. А.	Информационная безопасность. Введение в специальность + eПриложение: Тесты: Учебник	Москва: КноРус, 2021, URL: https://book.ru/book/936335
Л1.3	Клименко И.С.	Информационная безопасность и защита информации: модели и методы управления: Монография	Москва: ООО "Научно-издательский центр ИНФРА-М", 2021, URL: http://znanium.com/catalog/document?id=360289

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год
--	---------------------	----------	-------------------

	Авторы, составители	Заглавие	Издательство, год
Л2.1	Баранова Е.К., Бабаш А.В.	Информационная безопасность и защита информации: Учебное пособие	Москва: Издательский Центр РИО, 2021, URL: http://znanium.com/catalog/document?id=364911
Л2.2	Аверченков В.И.	Аудит информационной безопасности: Учебное пособие	Москва: Издательство "Флинта", 2011, URL: https://znanium.com/catalog/document?id=277964
6.2. Электронные учебные издания и электронные образовательные ресурсы			
Э1	Интернет университет информационных технологий ИНТУИТ https://www.intuit.ru/studies/courses		. - Режим доступа:
Э2	Естественно-научный образовательный портал. - Режим доступа:		http://www.en.edu.ru/
Э3	Федеральный центр информационно-образовательных ресурсов		. - Режим доступа: http://fcior.edu.ru/
Э4	Единое окно доступа к образовательным ресурсам Единое окно доступа к образовательным ресурсам. - Режим доступа: http://window.edu.ru		
Э5	Электронная библиотечная система Znanium. - Режим доступа: http://new.znanium.com/		
Э6	Электронная библиотечная система Ibooks. - Режим доступа: http://www.ibooks.ru		
Э7	Электронная библиотечная система BOOK.ru. - Режим доступа: http://www.book.ru		
Э8	Электронные ресурсы Академии ИМСИТ. - Режим доступа: http://eios.imsit.ru/		
Э9	Web-ресурс «Официальный сайт Академии ИМСИТ. - Режим доступа: http://imsit.ru		
6.3.1. Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства			
6.3.1.1	Windows 10 Pro RUS Операционная система – Windows 10 Pro RUS Подписка Microsoft Imagine Premium – Order №143659 от 12.07.2021		
6.3.1.2	7-Zip Архиватор 7-Zip Программное обеспечение по лицензии GNU GPL		
6.3.1.3	Яндекс Браузер Браузер Яндекс Браузер Лицензионное соглашение на использование программ Яндекс Браузер https://yandex.ru/legal/browser_agreement/		
6.3.1.4	Mozilla Firefox Браузер Mozilla Firefox Программное обеспечение по лицензии GNU GPL		
6.3.1.5	LibreOffice Офисный пакет LibreOffice Программное обеспечение по лицензии GNU GPL		
6.3.2. Перечень профессиональных баз данных и информационных справочных систем			
6.3.2.1	Кодекс – Профессиональные справочные системы https://kodeks.ru		
6.3.2.2	Консультант Плюс http://www.consultant.ru		

7. МТО (оборудование и технические средства обучения)

Ауд	Наименование	ПО	Оснащение
123	Кабинет информационной безопасности	Windows 10 Pro RUS 7-Zip Яндекс Браузер Mozilla Firefox LibreOffice LibreCAD Inkscape Notepad++. 1С:Предприятие 8. Комплект Kaspersky Endpoint Security MS Access 2016 MS Project Pro 2016 MS SQL Server 2019 MS SQL Server Management Studio 18.8 MS Visio Pro 2016 MS Visual Studio Community Edition Visual Studio Code Blender Gimp Maxima Oracle VM VirtualBox StarUML V1 PostgreSQL IntelliJ IDEA	Стол - 20 шт., стул - 21 шт., рабочее место преподавателя – 1 шт., персональный компьютер с выходом в интернет - 21 шт., доска учебная – 1 шт., многофункциональное устройство – 1 шт., мультимедийный проектор – 1 шт., проекционный экран – 1 шт., соответствующее программное обеспечение

		PyCharm Community Edition Eclips Adobe Reader DC Arduino Software (IDE) NetBeans IDE ZEAL ARIS Express Archimate Ramus Educational Micro-Cap Evaluation gvSIG Desktop Python	
208	Лаборатория Электротехники, электроники и схемотехники	Windows 10 Pro RUS 7-Zip Яндекс Браузер Mozilla Firefox LibreOffice LibreCAD Inkscape Notepad++. Kaspersky Endpoint Security MS Access 2016 MS Project Pro 2016 MS SQL Server 2019 MS SQL Server Management Studio 18.8 MS Visio Pro 2016 MS Visual Studio Community Edition Visual Studio Code Blender Gimp Maxima Oracle VM VirtualBox PostgreSQL IntelliJ IDEA PyCharm Community Edition Eclips Adobe Reader DC Diptrace Arduino Software (IDE) NetBeans IDE ZEAL NI LabVIEW Full Micro-Cap Evaluation Python	Стол - 10 шт., стул - 21 шт., рабочее место преподавателя - 1 шт., персональных компьютеров с выходом в интернет - 20 шт., доска учебная - 1 шт., многофункциональное устройство - 1 шт., мультимедийный проектор - 1 шт., проекционный экран - 1 шт., междисциплинарная лабораторная станция NI ELVIS II и ПО Circuit Design Suit - 1 шт, соответствующее программное обеспечение, учебно-лабораторные стенды для освоения типовых схемотехнических решений, контрольно-измерительная аппаратура для измерения временных характеристик, амплитуды и формы сигналов, генераторы сигналов с заданными параметрами, средства для измерения параметров электрических цепей - учебно-лабораторные стенды и контрольно-измерительная аппаратура для измерения частотных свойств, форм и временных характеристик сигналов, средства для измерения параметров электрических цепей, средства генерирования сигналов
Читальный зал	Информационно-библиотечный центр (помещение для самостоятельной работы обучающихся)	7-Zip Яндекс Браузер Mozilla Firefox LibreOffice LibreCAD Inkscape Notepad++. Kaspersky Endpoint Security MS Access 2016 MS Project Pro 2016 MS Visio Pro 2016 Visual Studio Code Blender Gimp Maxima IntelliJ IDEA PyCharm Community Edition Adobe Reader DC MS Office Standart 2007 Windows 10 Pro	Стол - 20 шт., стул - 20 шт., рабочее место сотрудника - 2 шт., персональный компьютер с выходом в интернет и обеспечением доступа в электронную информационно-образовательную среду академии - 17 шт., многофункциональное устройство - 2 шт.
235	Аудитория	7-Zip	Стол - 8 шт., стул - 20 шт., рабочее место преподавателя - 1

(защищаемое помещение) для проведения учебных занятий, с информацией ограниченного доступа, не содержащей сведений, составляющих государственную тайну	Яндекс Браузер Mozilla Firefox LibreOffice	шт., мультимедийный проектор (переносной) – 1 шт., переносной ноутбук – 1 шт., технические средства защиты
--	--	--

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

В соответствии с требованиями ФГОС ВО по направлению подготовки реализация компетентностного подхода предусматривает использование в учебном процессе активных и интерактивных форм проведения занятий (разбор конкретных задач, проведение блиц-опросов, исследовательские работы) в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

Лекционные занятия дополняются ПЗ и различными формами СРС с учебной и научной литературой. В процессе такой работы студенты приобретают навыки «глубокого чтения» - анализа и интерпретации текстов по методологии и методике дисциплины.

Учебный материал по дисциплине «Порядок проведения аттестации объектов информатизации». разделен на логически завершённые части (модули), после изучения, которых предусматривается аттестация в форме письменных тестов, контрольных работ.

Работы оцениваются в баллах, сумма которых дает рейтинг каждого обучающегося. В баллах оцениваются не только знания и навыки обучающихся, но и их творческие возможности: активность, неординарность решений поставленных проблем. Каждый модуль учебной дисциплины включает обязательные виды работ – лекции, ПЗ, различные виды СРС (выполнение домашних заданий по решению задач, подготовка к лекциям и практическим занятиям).

Форма текущего контроля знаний – работа студента на практическом занятии, опрос. Форма промежуточных аттестаций – контрольная работа в аудитории, домашняя работа. Итоговая форма контроля знаний по модулям – контрольная работа с задачами по материалу модуля.

Методические указания по выполнению всех видов учебной работы размещены в электронной образовательной среде академии.

Методические указания и материалы по видам учебных занятий по дисциплине:

Вид учебных занятий, работ - Организация деятельности обучающегося

Лекция - Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения, отмечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, попытаться найти ответ в рекомендуемой литературе, если самостоятельно не удастся разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии.

Практические занятия - Конспектирование источников. Работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы, работа с текстом. Выполнение практических задач в инструментальных средах. Выполнение проектов. Решение расчётно-графических заданий, решение задач по алгоритму и др.

Самостоятельная работа - Знакомство с основной и дополнительной литературой, включая справочные издания, зарубежные источники, конспект основных положений, терминов, сведений, требующихся для запоминания и являющихся основополагающими в этой теме. Составление аннотаций к прочитанным литературным источникам и др.

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ОБУЧАЮЩИМСЯ ПО ВЫПОЛНЕНИЮ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Методические указания по выполнению самостоятельной работы по дисциплине «Порядок проведения аттестации объектов информатизации».

Формой осуществления контроля выполнения самостоятельной работы является подготовка рефератов на актуальные темы,

т. е. изучение с помощью научных методов явлений и процессов, анализа влияния на них различных факторов, а также, изучение взаимодействия между явлениями, с целью получения убедительно доказанных и полезных для науки и практики решений с максимальным эффектом.

Цель реферата – определение конкретного объекта и всестороннее, достоверное изучение его структуры, характеристик, связей на основе разработанных в науке принципов и методов познания, а также получение полезных для деятельности человека результатов, внедрение в производство с дальнейшим эффектом.

Основой разработки каждой темы является методология, т. е. совокупность методов, способов, приемов и их определенная последовательность, принятая при разработке научного исследования. В конечном счете, методология – это схема, план решения поставленной научно исследовательской задачи.

Процесс подготовки реферата состоит из следующих основных этапов:

1. Выбор темы и обоснование ее актуальности.
2. Составление библиографии, ознакомление с законодательными актами, нормативными документами и другими источниками, относящимися к теме проекта (работы).

3. Разработка алгоритма исследования, формирование требований к исходным данным, выбор методов и инструментальных средств анализа.
4. Сбор фактического материала.
5. Обработка и анализ полученной информации с применением современных методов анализа.
6. Формулировка выводов и выработка рекомендаций.
7. Оформление работы в соответствии с установленными требованиями