

Министерство сельского хозяйства Российской Федерации

федеральное государственное бюджетное образовательное учреждение
высшего образования «Вологодская государственная молочнохозяйственная
академия имени Н.В. Верещагина»

Технологический факультет

Кафедра технологического оборудования

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

СОВРЕМЕННЫЕ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Направление подготовки (специальность): 27.04.01 Стандартизация и метрология

Профиль: Стандартизация и сертификация в пищевой отрасли

Квалификации выпускника: магистр

ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 27.04.01 Стандартизация и метрология.

Разработчик, к.т.н., доцент Виноградова Ю.В.

Рабочая программа одобрена на заседании кафедры технологического оборудования от «25» января 2024 года, протокол № 6.

Зав. кафедрой, к.т.н., доцент Кузин А.А.

Рабочая программа дисциплины согласована на заседании методической комиссии технологического факультета от «15» февраля 2024 года, протокол № 6.

Председатель методической комиссии, к.т.н., доцент Неронова Е.Ю.

1 Цели и задачи дисциплины

Целью изучения дисциплины «Современные информационно-коммуникационные технологии и информационная безопасность» является формирование у студентов системы знаний в области современных информационно-коммуникационных технологий, информационной безопасности и применения на практике методов и средств защиты информации.

Задачи дисциплины:

- Получение знаний о современных информационно-коммуникационных технологиях и сферах их применения в практической деятельности;
- Формирование умений в сфере обеспечения защиты информации и объектов информатизации; навыков выполнения работ в области защиты объектов интеллектуальной собственности и результатов исследований и разработок как коммерческой тайны предприятия; навыков настройки и обслуживания аппаратно-программных средств.

2 Место дисциплины в структуре ООП

Дисциплина «Современные информационно-коммуникационные технологии и информационная безопасность» является дисциплиной обязательной части дисциплин федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки 27.04.01 Стандартизация и метрология, профиль Стандартизация и сертификация в пищевой отрасли (Б1.О.06).

Области профессиональной деятельности и сферы профессиональной деятельности, в которых выпускники, освоившие программу магистратуры, могут осуществлять профессиональную деятельность:

01 Образование и наука (в сферах: реализации образовательных программ профессионального образования, высшего образования и дополнительного профессионального образования; научных исследований);

40 Сквозные виды профессиональной деятельности в промышленности (в сферах: обеспечения выпуска продукции, соответствующей требованиям нормативных документов и технических условий, эталонам, проектно-конструкторской и технологической документации; в сферах метрологического обеспечения производственной деятельности).

В рамках освоения образовательной программы выпускники могут готовиться к решению задач профессиональной деятельности следующих типов:

- научно-исследовательский;
- производственно-технологический;
- организационно-управленческий.

Объекты профессиональной деятельности: продукция (услуги) и технологические процессы; оборудование предприятий и организаций, метрологических и испытательных лабораторий; методы и средства измерений, испытаний и контроля; техническое регулирование, системы стандартизации, сертификации и управления качеством, метрологическое обеспечение научной, производственной, социальной и экологической деятельности; нормативная документация.

Для ее изучения необходимы знания, умения и компетенции в объеме, предусмотренном государственным образовательным стандартом высшего (полного) общего образования (уровень бакалавриата).

«Современные информационно-коммуникационные технологии и информационная безопасность» является предшествующей дисциплиной для последующего написания выпускной квалификационной работы.

3 Требования к результатам освоения дисциплины

Процесс изучения дисциплины «Современные информационно-коммуникационные технологии и информационная безопасность» направлен на формирование следующих компетенций бакалавра:

ОПК-9 Способен разрабатывать алгоритмы и программы, пригодные для практического применения в области профессиональной деятельности, с применением современных информационно-коммуникационных технологий и с учетом требований информационной безопасности

Код и наименование компетенции	Код и наименование индикатора достижения компетенции
ОПК-9 Способен разрабатывать алгоритмы и программы, пригодные для практического применения в области профессиональной деятельности, с применением современных информационно-коммуникационных технологий и с учетом требований информационной безопасности	ИД-1 ОПК-9 Знает требования информационной безопасности ИД-2 ОПК-9 Разрабатывает алгоритмы и программы для практического применения в области профессиональной деятельности ИД-3 ОПК-9 Применяет требования информационной безопасности при разработке алгоритмов программ для профессиональной деятельности

4 Структура и содержание учебной дисциплины

Общий объем дисциплины составляет 3 зачетных единицы.

4.1 Структура дисциплины

Вид учебной работы	Всего часов	Семестр
--------------------	-------------	---------

	(очно)	3
Аудиторные занятия (всего)	48	48
В том числе		
Лекции	16	16
Практические занятия	32	32
Семинары		
Лабораторные работы		
Самостоятельная работа (всего)	60	60
Контроль		
Вид промежуточной аттестации	Зачет	Зачет
Общая трудоёмкость часы	108	108
зачётные единицы	3	3

4.2 Содержание разделов дисциплины

Информационные процессы и цифровые технологии

Содержание информационных процессов и технологий. Структура информационной технологии. Классификация информационных технологий. Подсистемы информационных технологий. Цифровые прорывные технологии.

Программные средства реализации цифровых процессов

Программные средства реализации цифровых процессов. Уровни представления ПО. Операционные системы. Системы управления данными. Модели представления данных.

Цифровые технологии работы с графической информацией

Технологии работы с графической информацией. Растровая и векторная графика. Аппаратные средства ввода и вывода графических изображений. Прикладные программы работы с графикой. Графический редактор. Основные инструменты и режимы работы.

Передовые технологии XXI века: IoT, IoE, Cloud Computing, Artificial Intelligence и Machine Learning

Концепция IoT, IoE, Cloud Computing, Artificial Intelligence и Machine Learning, этапы развития технологий. Примеры их использования.

Организационное обеспечение информационной безопасности

Основные стандарты в области обеспечения информационной безопасности. Политика безопасности. Экономическая безопасность предприятия.

Технические средства и методы защиты информации

Инженерная защита объектов. Защита информации от утечки по техническим каналам. Симметричные и ассиметричные системы шифрования. Цифровые подписи (Электронные подписи). Инфраструктура открытых ключей. Криптографические протоколы.

Программно-аппаратные средства и методы обеспечения информационной безопасности

Основные виды сетевых и компьютерных угроз. Средства и методы защиты от сетевых компьютерных угроз. Создание зашифрованных файлов и криптоконтейнеров и их расшифрование.

Антивирусные средства защиты информации

Компьютерные вирусы: понятие, виды, особенности воздействия и распространения. Изучение настроек средств антивирусной защиты информации.

4.3 Разделы дисциплины и вид занятий

п/п	Наименование разделов учебной дисциплины	Лекции	Лабораторные занятия	СРС	Контроль	Всего часов
1	Информационные процессы и цифровые технологии	2	4	8		14
2	Программные средства реализации цифровых процессов	2	4	8		14
3	Цифровые технологии работы с графической информацией	2	4	8		14
4	Передовые технологии XXI века: IoT, IoE, Cloud Computing, Artificial Intelligence и Machine Learning	2	4	8		14
5	Организационное	2	4	8		14

	обеспечение информационной безопасности					
6	Технические средства и методы защиты информации	2	4	8		14
7	Программно-аппаратные методы и средства обеспечения информационной безопасности	2	4	8		14
8	Антивирусные средства защиты информации	2	4	4		10
Итого		16	32	60		108

5 Матрица формирования компетенций по дисциплине

№ п/п	Раздел дисциплины	Компетенции		Общее количество компетенций
		Общепрофессиональные		
		ОПК-9		
1	Информационные процессы и цифровые технологии		+	1
2	Программные средства реализации цифровых процессов		+	1
3	Технологии работы с графической информацией		+	1
4	Передовые технологии XXI века: IoT, IoE, Cloud Computing, Artificial Intelligence и Machine Learning		+	1
5	Организационное обеспечение информационной безопасности		+	1
6	Технические средства и методы защиты		+	1

	информации		
7	Программно-аппаратные методы и средства обеспечения информационной безопасности	+	1
8	Антивирусные средства защиты информации	+	1

6 Образовательные технологии

Объем аудиторных занятий: всего 68 часов, в том числе лекции 16 часов, практические занятия 32 часов, интерактивные занятия от общего объема аудиторных занятий составляют 100 %.

Семестр	Вид занятия (Л, ПЗ, ЛР)	Используемые интерактивные образовательные технологии	Количество часов
13	Л	Лекция-визуализация на тему: «Информационные процессы и цифровые технологии»	2
	Л	Лекция-визуализация на тему: «Программные средства реализации цифровых процессов»	2
	Л	Лекция-визуализация на тему: «Технологии работы с графической информацией»	2
	Л	Лекция-визуализация на тему: «Передовые технологии XXI века: IoT, IoE, Cloud Computing, Artificial Intelligence и Machine Learning»	2
	Л	Лекция-визуализация на тему: «Организационное обеспечение информационной безопасности»	2
	Л	Лекция-визуализация на тему: «Технические средства и методы защиты информации»	2
	Л	Лекция-визуализация на тему: «Программно-аппаратные методы и средства обеспечения информационной безопасности»	2
	Л	Лекция-визуализация на тему: «Антивирусные средства защиты информации»	2

ПЗ	Технологии обработки текстовой информации. Продвинутый уровень.	4
ПЗ	Обработка числовых данных в цифровом пространстве. Продвинутый уровень	4
ПЗ	Создание графической документации в системах автоматизированного проектирования	4
ПЗ	Обзор и практическое использование облачных сервисов	4
ПЗ	Case-study «Понятие и сущность защиты информации и ее место в системе информационной безопасности»	4
ПЗ	Case-study «Криптографические методы защиты информации»	4
ПЗ	Case-study «Использование цифровых подписей»	4
ПЗ	Case-study «Перекрытие каналов несанкционированного доступа к источникам конфиденциальной информации»	4
Итого		68

7 Учебно-методическое обеспечение самостоятельной работы студентов. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

7.1 Виды самостоятельной работы, порядок их выполнения и контроля

№ п/п	Раздел дисциплины	Виды СРС	Порядок выполнения СРС	Метод контроля
1	Информационные процессы и цифровые технологии	Подготовка к тестированию, устному опросу	Работа с лекционным материалом, основной и дополнительной литературой, Интернет-ресурсами	Устный опрос, Тестирование
2	Программные средства реализации цифровых процессов	Подготовка к тестированию, устному	Работа с лекционным материалом, основной и дополнительной	Устный опрос, Тестирование

		опросу	литературой, Интернет-ресурсами	
3	Технологии работы с графической информацией	Подготовка к тестированию, устному опросу	Работа с лекционным материалом, основной и дополнительной литературой, Интернет-ресурсами	Устный опрос, Тестирование
4	Передовые технологии XXI века: IoT, IoE, Cloud Computing, Artificial Intelligence и Machine Learning	Подготовка к тестированию, устному опросу	Работа с лекционным материалом, основной и дополнительной литературой, Интернет-ресурсами, индивидуальная работа	Устный опрос, Тестирование
5	Организационное обеспечение информационной безопасности	Подготовка к тестированию, устному опросу	Работа с лекционным материалом, основной и дополнительной литературой, Интернет-ресурсами	Устный опрос, Тестирование
6	Технические средства и методы защиты информации	Подготовка к тестированию, устному опросу	Работа с лекционным материалом, основной и дополнительной литературой, Интернет-ресурсами, индивидуальная работа	Устный опрос, Тестирование
7	Программно-аппаратные методы и средства	Подготовка к тестированию, устному	Работа с лекционным материалом,	Устный опрос, Тестирование

	обеспечения информационной безопасности	опросу	основной и дополнительной литературой, Интернет-ресурсами	
8	Антивирусные средства защиты информации	Подготовка к тестированию, устному опросу	Работа с лекционным материалом, основной и дополнительной литературой, Интернет-ресурсами	Устный опрос, Тестирование

7.2 Контрольные вопросы для самопроверки

1. Что такое информационная безопасность?
2. Перечислите основные угрозы информационной безопасности.
3. Какие существуют модели информационной безопасности?
4. Какие методы защиты информации выделяют?
5. Что такое правовые методы защиты информации?
6. Что такое организационные методы защиты информации?
7. Что такое технические методы защиты информации?
8. Что такое программно-аппаратные методы защиты информации?
9. Что такое криптографические методы защиты информации?
10. Что такое физические методы защиты информации?
11. Какие главные государственные органы в области обеспечения информационной безопасности?
12. Перечислите виды защищаемой информации.
13. Какие основные законы в области защиты информации в РФ?
14. Перечислите основные цели и задачи РФ в области обеспечения информационной безопасности
15. Что такое концепция информационной безопасности?
16. Что такое конфиденциальная информация?
17. Что такое персональные данные?
18. В каких случаях возможно использовать персональные данные без согласия обладателя?
19. Охарактеризуйте биометрические данные как персональные данные.
20. Что такое профессиональная тайна?
21. Что такое коммерческая тайна?

22. Что такое режим коммерческой тайны?
23. Что такое государственная тайна?
24. Опишите правовой режим государственной тайны.
25. Какие государственные органы занимаются сертификацией и лицензированием средств защиты информации?
26. Тема 3. Организационное обеспечение информационной безопасности
27. Какие основные международные стандарты в области информационной безопасности существуют?
28. Как связаны международные стандарты и стандарты РФ?
29. Какие основные стандарты РФ в области информационной безопасности существуют?
30. Охарактеризуйте стандарт ГОСТ Р ИСО/МЭК 27002-2014.
31. Что такое политика безопасности?
32. Какое количество средств бюджета организации эффективно тратить для обеспечения информационной безопасности?
33. Что такое инженерная защита объектов?
34. Какие виды сигнализаций устанавливаются для обеспечения инженерной защиты?
35. Что такое технические каналы утечки информации?
36. Перечислите основные виды технических каналов утечки информации?
37. Перечислите методы защиты информации от утечки по визуаль-ному каналу.
38. Перечислите методы защиты информации от утечки по воздуш-ному каналу.
39. Перечислите методы защиты информации от утечки по вибраци-онному каналу.
40. Перечислите методы защиты информации от утечки по индук-ционному каналу.
41. Перечислите средства и методы защиты информации от утечки в телефонных линиях.
42. Перечислите основные мероприятия по обеспечению защиты информации от утечки по техническим каналам.
43. Какие виды компьютерных угроз существуют?
44. Что такое брандмауэр?
45. Что такое антивирусная программа?
46. Что такое эвристический алгоритм поиска вирусов?
47. Что такое сигнатурный поиск вирусов?
48. Методы противодействия сниффингу?
49. Какие программные реализации программно-аппаратных средств защиты информации вы знаете?
50. Что такое механизм контроля и разграничения доступа?

51. Какую роль несет журналирование действий в программно-аппаратных средствах защиты информации?
52. Что такое средства стеганографической защиты информации?
53. Что такое криптография?
54. Какие используются симметричные алгоритмы шифрования?
55. Какие используются ассиметричные алгоритмы шифрования?
56. Что такое криптографическая хеш-функция?
57. Какие используются криптографические хеш-функции?
58. Что такое цифровая подпись?
59. Что такое инфраструктура открытых ключей?
60. Какие российские и международные стандарты на формирование цифровой подписи существуют?
61. Какие основные криптографические протоколы используются в сетях?

7.3 Вопросы для промежуточной аттестации

1. Цели государства в области обеспечения информационной безопасности.
2. Основные нормативные акты РФ, связанные с правовой защитой информации.
3. Виды компьютерных преступлений.
4. Способы и механизмы совершения информационных компьютерных преступлений.
5. Основные параметры и черты информационной компьютерной преступности в России.
6. Компьютерный вирус. Основные виды компьютерных вирусов.
7. Методы защиты от компьютерных вирусов.
8. Типы антивирусных программ.
9. Защиты от несанкционированного доступа. Идентификация и аутентификация пользователя.
10. Основные угрозы компьютерной безопасности при работе в сети Интернет.
11. Виды защищаемой информации.
12. Государственная тайна как особый вид защищаемой информации.
13. Конфиденциальная информация.
14. Система защиты государственной тайны.
15. Правовой режим защиты государственной тайны.
16. Защита интеллектуальной собственности средствами патентного и авторского права.
17. Международное законодательство в области защиты информации.
18. Программно-аппаратные средства обеспечения информационной безопасности в информационных сетях.
19. Симметричные шифры.

20. Ассиметричные шифры.
21. Криптографические протоколы.
22. Криптографические хеш-функции.
23. Электронная подпись.
24. Организационное обеспечение информационной безопасности.
25. Служба безопасности организации.
26. Методы защиты информации от утечки в технических каналах.
27. Инженерная защита и охрана объектов.

8 Учебно-методическое и информационное обеспечение дисциплины (модуля)

а) основная литература

1. Петров, А. А. Компьютерная безопасность. Криптографические методы защиты : практическое руководство / А. А. Петров. - 2-е изд. - Москва : ДМК Пресс, 2023. - 451 с. - ISBN 978-5-89818-453-7. - Текст : электронный. - URL: <https://znanium.com/catalog/product/2106222> (дата обращения: 02.12.2023). – Режим доступа: по подписке.

2. Информационные системы и цифровые технологии [Электронный ресурс] : учебное пособие : в 2-х частях. Ч. 1 / В. В. Трофимов, М. И. Барабанова, В. И. Кияев, Е. В. Трофимова ; под ред. В. В. Трофимова, В. И. Кияева. - Электрон.дан. - Санкт-Петербург : СПбГЭУ, 2021. - 253 с. - Внешняя ссылка: <http://znanium.com/catalog/document?id=375739>

3. Информационные системы и цифровые технологии [Электронный ресурс] : учебное пособие : в 2-х частях. Ч. 2 / М. И. Барабанова, В. Ф. Минаков, Т. А. Макаrchук [и др.] ; под ред. В. В. Трофимова, В. И. Кияева. - Электрон.дан. - Москва : ИНФРА-М, 2021. - 270 с. - Внешняя ссылка: <http://znanium.com/catalog/document?id=382228>

4. Информационная безопасность и защита информации [Электронный ресурс] : учебное пособие / Е. К. Баранова, А. В. Бабаш. - 4-е изд., перераб. и доп. - Электрон.дан. - Москва : РИОР : ИНФРА-М, 2021. - 336 с. - (Высшее образование). - Внешняя ссылка: <http://znanium.com/catalog/document?id=364911>

5. Защита информации и информационная безопасность [Электронный ресурс] : учебное пособие / Ю. Н. Сычев. - Электрон.дан. - Москва : ИНФРА-М, 2021. - 201 с. - Внешняя ссылка: <http://znanium.com/catalog/document?id=365029>

б) дополнительная литература

1. Комплексная защита информации в корпоративных системах [Электронный ресурс] : учебное пособие / В. Ф. Шаньгин. - Электрон.дан. -

Москва : ФОРУМ : ИНФРА-М, 2020. - 592 с. - Внешняя ссылка:
<http://znanium.com/catalog/document?id=358722>

2. Борисова, Н. А. Основы построения инфокоммуникационных систем и сетей : учебное пособие / Н. А. Борисова, В. Ю. Гойхман. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2018. — 120 с. — ISBN 978-5-89160-176-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/180144> — Режим доступа: для авториз. пользователей.

3. Голиков, А. М. Защита информации в инфокоммуникационных системах и сетях : учебное пособие / А. М. Голиков. — Москва : ТУСУР, 2015. — 284 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/110336> — Режим доступа: для авториз. пользователей.

в) Перечень информационных технологий и программного обеспечения, используемых при изучении дисциплины

Лицензионное программное обеспечение:

Microsoft Windows XP / Microsoft Windows 7 Professional , Microsoft Office Professional 2003 / Microsoft Office Professional 2007 / Microsoft Office Professional 2010

STATISTICA Advanced + QC 10 for Windows

в т.ч. отечественное

Astra Linux Special Edition РУСБ 10015-01 версии 1.6.

1С:Предприятие 8. Конфигурация, 1С: Бухгалтерия 8 (учебная версия)

Project Expert 7 (Tutorial) for Windows

СПС КонсультантПлюс

Kaspersky Endpoint Security для бизнеса Стандартный

Свободно распространяемое лицензионное программное обеспечение:

OpenOffice

LibreOffice

7-Zip

Adobe Acrobat Reader

Google Chrome

в т.ч. отечественное

Яндекс.Браузер

Информационные справочные системы

– [Единое окно доступа к образовательным ресурсам](http://window.edu.ru/) – режим доступа:
<http://window.edu.ru/>

– ИПС «КонсультантПлюс» – режим доступа: <http://www.consultant.ru/>

- Интерфакс - Центр раскрытия корпоративной информации (сервер раскрытия информации) – режим доступа: <https://www.e-disclosure.ru/>
- Информационно-правовой портал ГАРАНТ.RU – режим доступа: <http://www.garant.ru/>
- Автоматизированная справочная система «Сельхозтехника» (web-версия) - режим доступ: <http://gtexam.ru/>

Профессиональные базы данных

- Научная электронная библиотека eLIBRARY.RU – режим доступа: <http://elibrary.ru>
- Наукометрическая база данных Scopus: база данных рефератов и цитирования – режим доступа: <https://www.scopus.com/customer/profile/display.uri>
- Официальный сайт Федеральной службы государственной статистики – режим доступа: <https://rosstat.gov.ru/> (Открытый доступ)
- Российская Академия Наук, открытый доступ к научным журналам – режим доступа: <http://www.ras.ru> (Открытый доступ)
- Официальный сайт Министерства сельского хозяйства Российской Федерации – режим доступа: <http://mex.ru/> (Открытый доступ)

Электронные библиотечные системы:

- Электронный библиотечный каталог Web ИРБИС – режим доступа: https://molochnoe.ru/cgi-bin/irbis64r_14/cgiirbis_64.exe?C21COM=F&I21DBNAM=STATIC&I21DBN=STATIS
- ЭБС ЛАНЬ – режим доступа: <https://e.lanbook.com/>
- ЭБС Znanium.com – режим доступа: <https://new.znaniy.com/>
- ЭБС ЮРАЙТ – режим доступа: <https://urait.ru/>
- ЭБС POLPRED.COM: <http://www.polpred.com/>
- Электронная библиотека издательского центра «Академия»: <https://www.academia-moscow.ru/elibrary/> (коллекция СПО)
- ЭБС ФГБОУ ВО Вологодская ГМХА – режим доступа: <https://molochnoe.ru/ebs/>

9. Материально-техническое обеспечение дисциплины

При изучении дисциплины используются:

1. стандартно оборудованные мультимедийные лекционные аудитории для проведения интерактивных лекций: компьютер, видеопроектор, экран настенный.
2. компьютерные классы с мультимедийным оборудованием;
3. компьютерные классы.

Программное обеспечение: Microsoft Windows 7 Professional, Лицензии 49230531, бессрочно

ОБЕСПЕЧЕНИЕ ОБРАЗОВАНИЯ ДЛЯ ЛИЦ С ОВЗ

Для обеспечения образования инвалидов и лиц с ограниченными возможностями здоровья реализация дисциплины может осуществляться в адаптированном виде, исходя из индивидуальных психофизических особенностей и по личному заявлению обучающегося, в части создания специальных условий.

В специальные условия могут входить: предоставление отдельной аудитории, необходимых технических средств, присутствие ассистента, оказывающего необходимую техническую помощь, выбор формы предоставления инструкции по порядку проведения текущего контроля и промежуточной аттестации, использование специальных технических средств, предоставление перерыва для приема пищи, лекарств и др.

Для лиц с ограниченными возможностями здоровья предусмотрена организация консультаций с использованием электронной почты.

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

- в печатной форме увеличенным шрифтом,
- в форме электронного документа.

Для лиц с нарушениями слуха:

- в печатной форме,
- в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

- в печатной форме,
- в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

10 Перечень компетенций, этапы, показатели и критерии оценивания

Название дисциплины (код и название направления подготовки) Современные информационно-коммуникационные технологии и информационная безопасность (направление подготовки 27.04.01 Стандартизация и метрология)					
Цель дисциплины	формирование у студентов системы знаний в области современных информационно-коммуникационных технологий, информационной безопасности и применения на практике методов и средств защиты информации.				
Задачи дисциплины	Получение знаний о современных информационно-коммуникационных технологиях и сферах их применения в практической деятельности; формирование умений обеспечения защиты информации и объектов информатизации; навыков выполнения работ в области защиты объектов интеллектуальной собственности и результатов исследований и разработок как коммерческой тайны предприятия; навыков настройки и обслуживания аппаратно-программных средств.				
В процессе освоения данной дисциплины студент формирует и демонстрирует следующие					
Компетенции		Перечень компонентов (индикаторы достижения компетенции)	Технологии формирования	Форма оценочного средства	Ступени уровней освоения компетенции
Индекс	Формулировка				
ОПК-9	Способен разрабатывать алгоритмы и программы, пригодные для практического применения в области профессиональной деятельности, с	ИД-1 ОПК-9 Знает требования информационной безопасности ИД-2 ОПК-9 Разрабатывает алгоритмы и программы для практического применения в области профессиональной деятельности ИД-3 ОПК-9 Применяет	Лекции Практические занятия Самостоятельная работа	Тестирование Устный опрос	Пороговый (удовлетворительный) От 30-50 баллов Знает требования информационной безопасности Продвинутый (хорошо) От 51-80 баллов Разрабатывает алгоритмы и программы для практического применения в области
Высокий					

	<p>применением современных информационно-коммуникационных технологий и с учетом требований информационной безопасности</p>	<p>требования информационной безопасности при разработке алгоритмов программ для профессиональной деятельности</p>			<p>(отлично) От 81-100 баллов Применяет требования информационной безопасности при разработке алгоритмов программ для профессиональной деятельности</p>
--	--	--	--	--	---

СОДЕРЖАНИЕ

1 Цели и задачи дисциплины

2 Место дисциплины в структуре ООП

3 Требования и результаты освоения дисциплины

4 Структура и содержание дисциплины

5 Матрица формирования компетенций по дисциплине

6 Образовательные технологии

7 Учебно-методическое обеспечение самостоятельной работы студентов. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

8 Учебно-методическое и информационное обеспечение дисциплины

9 Материально-техническое обеспечение дисциплины

10 Перечень компетенций, этапы, показатели и критерии оценивания