ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СТАВРОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ

Директор/Декан
факультета цифровых технологий
Шлаев Дмитрий Валерьевич

_____

_____

«___» _____ 20___ г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ (ОЦЕНОЧНЫХ МАТЕРИАЛОВ)

Б1.О.27 Информационная безопасность

09.03.02 Информационные системы и технологии

Инженерия информационных систем

бакалавр

очная

Ставрополь, 2026

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

Процесс изучения дисциплины направлен на формирование следующих компетенций ОП ВО и овладение следующими результатами обучения по дисциплине:

Код и наименование компетенции	Код и наименование индикатора достижения	Перечень планируемых результатов обучения по дисциплине
ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3.1 Выбирает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**знает** информационно-законодательную базу для формирования политики информационной безопасности; административный и процедурный уровень информационной безопасности
		умеет решать аргументировано задачи политики информационной безопасности, анализировать угрозы информационной безопасности
		владеет навыками навыками информационной безопасности информационной и библиографической культуры с применением информационно- коммуникационных технологий и с учетом основных требований информационной безопасности
ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом	ОПК-3.2 Решает стандартные задачи профессиональной деятельности на основе информационной и	**знает** источники получения информационных данных необходимых для решения профессиональных задач; типовые методики организации коммуникаций; решение профессиональных задач в области информационной безопасности
		умеет анализировать угрозы и каналы утечки информации; выявлять тенденции изменения требований к информационной безопасности на предприятии

основных требований информационной безопасности	библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**владеет навыками** навыками информационной безопасности информационной и библиографической культуры с применением информационно- коммуникационных технологий и с учетом основных требований информационной безопасности
ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3.3 Участвует в подготовке обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	**знает** проблемы информационной безопасности и защиты информации
		умеет анализировать и давать критическую оценку решению научно-исследовательских задач в области информационной безопасности
		владеет навыками оформлением руководящих документов по информационной безопасности и защиты информации; методами представления предложений информационной безопасности в системах обработки данных

2. Перечень оценочных средств по дисциплине

№	Наименование раздела/темы	Семестр	Код индикаторов достижения компетенций	Оценочное средство проверки результатов достижения индикаторов компетенций
1.	1 раздел. 1			
1.1.	Общая характеристика информационной безопасности. Угроза (утечка) информации	3	ОПК-3.1, ОПК-3.2, ОПК-3.3	Тест
1.2.	Уровни информационной безопасности	3	ОПК-3.1, ОПК-3.2, ОПК-3.3	Устный опрос

1.3.	Политика информационной без-опасности и формирование методов защиты информационных ресурсов	3	ОПК-3.1, ОПК-3.2, ОПК-3.3	Устный опрос
	Промежуточная аттестация			Эк

3. Оценочные средства (оценочные материалы)

Примерный перечень оценочных средств для текущего контроля успеваемости и промежуточной аттестации

№ п/п	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде (Оценочные материалы)
Текущий контроль			
	Для оценки знаний		
1	Устный опрос	Средство контроля знаний студентов, способствующее установлению непосредственного контакта между преподавателем и студентом, в процессе которого преподаватель получает широкие возможности для изучения индивидуальных особенностей усвоения студентами учебного материала.	Перечень вопросов для устного опроса
2	Тест	Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося.	Фонд тестовых заданий
	Для оценки умений		
	Для оценки навыков		
	Промежуточная аттестация		
3	Экзамен	Средство контроля усвоения учебного материала и формирования компетенций, организованное в виде беседы по билетам с целью проверки степени и качества усвоения изучаемого материала, определить необходимость введения изменений в содержание и методы обучения.	Комплект экзаменационных билетов

4. Примерный фонд оценочных средств для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине (модулю) "Информационная безопасность"

Примерные оценочные материалы для текущего контроля успеваемости

Примерные оценочные материалы
для проведения промежуточной аттестации (зачет, экзамен)
по итогам освоения дисциплины (модуля)

Вопросы для подготовки к экзамену

1. Дайте характеристику понятие секретной информации.
2. Охарактеризуйте понятие коммерческой тайны.
3. Что такое разрушение информации?
4. Методы уменьшения опасности компьютерных вирусов.
5. Классификация информации по уровню доступа.
6. Что такое открытая информация?
7. Что такое информация ограниченного доступа?
8. Конфиденциальность информации.
9. Целостность информации.
10. Доступность информации.
11. Понятие информационной безопасности.
12. Основные составляющие информационной безопасности.
13. Законодательный уровень информационной безопасности.
14. Обзор российского законодательства в области информационной безопасности.
15. Обзор зарубежного законодательства в области информационной безопасности.
16. Основные классы мер процедурного уровня.
17. Информационная инфраструктура.
18. Основные классы мер процедурного уровня.
19. Физическая защита.
20. Критичные ресурсы.
21. Реагирование на нарушения режима безопасности.
22. Основные понятия административного уровня ИБ.
23. Программа безопасности.
24. Политика безопасности.
25. Политика безопасности нижнего уровня.
26. Синхронизация программы безопасности с жизненным циклом систем.
27. Контроль деятельности в области безопасности.
28. Охарактеризуйте понятие АС.
29. Охарактеризуйте информационную безопасность.
30. Охарактеризуйте понятие угрозы информационной безопасности.
31. Классификация угроз по природе возникновения.
32. Классификация угроз по степени преднамеренности возникновения.
33. Классификация угроз по положению источника.
34. Классификация угроз по степени воздействия на АС.
35. Технические каналы утечки информации.
36. Функциональные каналы утечки информации и условия их образования.
37. Специальные каналы утечки информации и механизмы их возникновения.
38. Процедурный уровень информационной безопасности.
39. Физическая защита информации.
40. Анализ угроз ИБ объекта.
41. Методы и средства обеспечения ИБ на объектах связи специального назначения.
42. Модели нарушителя и угроз безопасности объекта.
43. Методы и средства ограничения доступа к информации и компонентам ЭВМ.
44. Привязка программного обеспечения к аппаратному окружения и физическим носителям.
45. Защита компьютерной информации и компьютерных систем от вредоносных программ.
46. История криптографии.
47. Простейшие шифры и их свойства. Стойкость шифров. Композиции шифров. Влияние криптографических средств на информационную безопасность.
48. Проблемы и методы информационной войны.
49. Методы иностранных технических разведок по ведению информационной войны их возможности.

Темы письменных работ (эссе, рефераты, курсовые работы и др.)