ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
СТАВРОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ

C=RU, S=Ставропольский край, L=г. Ставрополь, T=проректор по учебной работе, OU=ректорат, O="ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ ""СТАВРОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ""", СНИЛС=15230589951, ИНН=263411176761, E=s.a.maksimovich@stgau.ru, G=Светлана Александровна, SN=Максимович, CN=Максимович Светлана Александровна

УТВЕРЖДАЮ

Директор/Декан
факультета цифровых технологий
Шлаев Дмитрий Валерьевич

_____

_____

«___» _____ 20___ г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ (ОЦЕНОЧНЫХ МАТЕРИАЛОВ)

Б1.В.05 Управление информационной безопасностью

09.04.03 Прикладная информатика

Искусственный интеллект в кибербезопасности

магистр

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
ПК-4 Способен администрировать средства защиты информации и обеспечивать безопасность информационных систем	ПК-4.1 Администрирует средства защиты информации прикладного и системного программного обеспечения (ОС, СУБД, приложения), настраивая политики безопасности и контролируя их соблюдение	**знает** средства защиты информации прикладного и системного программного обеспечения, политики информационной безопасности и порядок контроля их соблюдения
		умеет настраивать политики информационной безопасности и администрировать средства защиты информации
		владеет навыками навыками администрирования средств защиты информации и контроля соблюдения политик безопасности

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	1	ПК-4.1	Тест
1.2.	Уровни информационной безопасности	1	ПК-4.1	Тест
1.3.	Политика информационной без-опасности и формирование методов защиты информационных ресурсов	1	ПК-4.1	Тест
	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	Тест	Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося.	Фонд тестовых заданий
	Для оценки умений		
	Для оценки навыков		
	Промежуточная аттестация		
2	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) "Управление информационной безопасностью"

Примерные оценочные материалы для текущего контроля успеваемости

Примерные вопросы для устного опроса:

1. Что понимается под управлением информационной безопасностью?
2. Какие задачи решает политика информационной безопасности?
3. Какие средства защиты информации применяются в информационных системах?
4. Как выполняется настройка политик безопасности?
5. Для чего применяется контроль соблюдения политик безопасности?
6. Какие угрозы возникают при нарушении требований информационной безопасности?
7. Как организуется управление доступом пользователей?
8. Какие средства защиты применяются для операционных систем?
9. Как обеспечивается безопасность прикладного программного обеспечения?
10. Какую роль играет мониторинг событий информационной безопасности?
11. Как оценивается эффективность средств защиты информации?
12. Как искусственный интеллект может использоваться в управлении информационной безопасностью?

Примерные тестовые задания:

1. Политика информационной безопасности предназначена для:
а) установления правил защиты информации и порядка их соблюдения;
б) удаления всех информационных ресурсов;
в) отказа от контроля доступа;
г) замены всех пользователей.
Правильный ответ: а.

2. Администрирование средств защиты информации включает:

а) настройку, сопровождение и контроль работы защитных механизмов;
б) только удаление программного обеспечения;
в) отказ от обновлений;
г) отключение всех средств защиты.
Правильный ответ: а.

3. Контроль соблюдения политик безопасности необходим для:
а) выявления нарушений и поддержания защищенности информационных систем;
б) отмены требований безопасности;
в) передачи паролей всем пользователям;
г) удаления журналов событий.
Правильный ответ: а.

4. Управление доступом пользователей направлено на:
а) разграничение прав доступа к информационным ресурсам;
б) открытие всех данных для всех пользователей;
в) удаление учетных записей без анализа;
г) отказ от идентификации.
Правильный ответ: а.

5. Мониторинг событий информационной безопасности используется для:
а) обнаружения подозрительной активности и нарушений безопасности;
б) замены всех документов;
в) удаления средств защиты;
г) отключения информационной системы.
Правильный ответ: а.

Примерные практические задания:

1. Составить структуру политики информационной безопасности организации.
2. Определить требования к настройке политик безопасности для информационной системы.
3. Описать порядок администрирования средств защиты информации.
4. Составить схему разграничения доступа пользователей к информационным ресурсам.
5. Проанализировать возможные нарушения политики информационной безопасности.
6. Предложить меры контроля соблюдения требований безопасности.
7. Составить перечень событий, подлежащих мониторингу в системе безопасности.
8. Оценить возможности применения искусственного интеллекта для контроля информационной безопасности.

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.)

1. Управление информационной безопасностью в современных организациях.
2. Политика информационной безопасности: назначение, структура и содержание.
3. Администрирование средств защиты информации прикладного программного обеспечения.
4. Администрирование средств защиты информации системного программного обеспечения.
5. Настройка политик безопасности в информационных системах.
6. Контроль соблюдения требований информационной безопасности.
7. Управление доступом пользователей к информационным ресурсам.
8. Средства защиты операционных систем, баз данных и приложений.
9. Организация мониторинга событий информационной безопасности.
10. Риски нарушения политик информационной безопасности.
11. Методы оценки эффективности средств защиты информации.
12. Документирование процессов управления информационной безопасностью.
13. Роль искусственного интеллекта в управлении информационной безопасностью.
14. Автоматизация контроля соблюдения политик безопасности.
15. Совершенствование системы управления информационной безопасностью организации.