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.28 Программно-аппаратная защита информации

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** принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной библиографической культуры
		умеет решать стандартные задачи профессиональной деятельности с применением информационно-коммуникационных технологий
		владеет навыками методами и средствами информационной библиографической культуры для решения стандартных профессиональных задач
ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных	ОПК-3.2 Решает стандартные задачи профессиональной деятельности на основе информацион	**знает** основные требования информационной безопасности для решения стандартных задач профессиональной деятельности
		умеет решать стандартные задачи профессиональной деятельности с применением информационно-коммуникационных технологий и библиографической культуры

технологий и с учетом основных требований информационной безопасности	ной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**владеет навыками** методами и средствами информационной библиографической культуры для решения профессиональных задач с учётом 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** основные требования информационной безопасности при выполнении научно-исследовательской работы
		умеет участвовать в подготовке обзоров, аннотаций, рефератов, научных докладов, публикаций и библиографии
		владеет навыками методами и навыками оформления научных работ (обзоров, аннотаций, рефератов, докладов, библиографии) в соответствии с требованиями информационной безопасности
ОПК-5 Способен инсталлировать программное и аппаратное обеспечение для информационных и автоматизированных систем	ОПК-5.2 Успешно выполняет параметрическую настройку и инсталляцию программного и аппаратного обеспечения информационных и автоматизированных систем	**знает** методы и технологии параметрической настройки и инсталляции программного и аппаратного обеспечения информационных и автоматизированных систем
		умеет выполнять параметрическую настройку и установку программного и аппаратного обеспечения автоматизированных систем
		владеет навыками технологиями параметрической настройки и инсталляции программно-аппаратного обеспечения информационных систем
ОПК-5 Способен инсталлировать программное и аппаратное обеспечение для информационных и	ОПК-5.3 Применяет методики инсталляции программного	**знает** методики инсталляции программного обеспечения, установки и тестирования аппаратного обеспечения для интеллектуальных информационных и автоматизированных систем

автоматизированных систем	обеспечения, методики установки и тестирования аппаратного обеспечения для интеллектуальных, информационных и автоматизированных систем	**умеет** применять методики установки программного обеспечения и методики установки/тестирования аппаратного обеспечения
		владеет навыками методиками инсталляции, настройки и тестирования программно-аппаратного обеспечения для интеллектуальных информационных и автоматизированных систем
ОПК-7 Способен осуществлять выбор платформ и инструментальных программно-аппаратных средств для реализации информационных систем	ОПК-7.1 Обоснованно выбирает архитектурные решения для реализации информационных систем; платформу для разработки инфокоммуникационных систем	**знает** рхитектурные решения и платформы для реализации информационных систем и разработки телекоммуникационных систем
		умеет обоснованно выбирать архитектурные решения и платформы для реализации информационных и телекоммуникационных систем
		владеет навыками методами выбора архитектурных решений и платформ для разработки и реализации информационных и коммуникационных систем

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.	Программно-аппаратная защита ин-формации, основные понятия, определения, возможности использования.	3	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-5.2, ОПК-5.3, ОПК-7.1	Устный опрос
1.2.	КТ 1	3	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-5.2, ОПК-5.3, ОПК-7.1	Тест
1.3.	Методы и средства программно-аппаратных средства защиты ин-формации.	3	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-5.2, ОПК-5.3, ОПК-7.1	Устный опрос

1.4.	КТ 2	3	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-5.2, ОПК-5.3, ОПК-7.1	Тест
	Промежуточная аттестация			За

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	Зачет	Средство контроля усвоения учебного материала практических и семинарских занятий, успешного прохождения практик и выполнения в процессе этих практик всех учебных поручений в соответствии с утвержденной программой с выставлением оценки в виде «зачтено», «незачтено».	Перечень вопросов к зачету

4. Примерный фонд оценочных средств для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине (модулю) "Программно-аппаратная защита информации"

Примерные оценочные материалы для текущего контроля успеваемости

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

1. Несанкционированное копирование программ как особый вид НСД. понятие злоумышленника. Понятие злоумышленника в криптографии. Понятие злоумышленника в решении проблем компьютерной безопасности.
2. Конфиденциальность. Уровни (грифы) конфиденциальности по известным классификациям. Способы защиты конфиденциальности в компьютерных системах.
3. Понятия целостности и доступности информации. Способы защиты целостности и доступности информации в компьютерных системах.
4. Политики безопасности в компьютерных системах. Охватываемые политиками безопасности аспекты защиты. Выработка требований к политике безопасности для конкретной организации.
5. Полномочная политика безопасности, сущность и содержание, достоинства и недостатки.
6. Механизмы защиты, входящие в состав компьютерной системы, их свойства.
7. Руководящие документы ФСТЭК по оценке защищенности от НСД, состав, назначение.
8. Принципы реализации политики безопасности, их характеристики.
9. Понятие и основная задача идентификации пользователя. Понятие протокола идентификации. Локальная и удалённая идентификация.
10. Технология взаимной проверки подлинности пользователей.
11. Шифрование. Основные понятия, связанные с шифрованием. Роль шифрования в защите данных от несанкционированного доступа.
12. Разграничение доступа к файлам. Основные понятия. Система разграничения доступа к файлам.
13. Опишите состав системы разграничения доступа к файлам. Основная концепция, лежащая в основе построения системы разграничение доступа.
14. Организация доступа к файлам в серверных и настольных ОС семейства Microsoft Windows.
15. Что такое фиксация доступа к файлам. Задачи и способы фиксации и записи фактов доступа к файлам.
16. Что такое электронные журналы доступа к файлам, их назначение, критерии информативности журналов доступа.
17. Следы несанкционированного доступа к файлам. Способы выявления следов несанкционированного доступа к файлам. Способы удаления или сведения к минимуму следов доступа к файлам злоумышленником.
18. Надежность систем ограничения доступа, понятие и основные слагаемые надёжности.
19. Целостность информации. Имитозащита. Подход к защите данных на основании формирования имитовставки (имитоприставки). Требования к имитовставке. Способы построения имитовставки.
20. Подходы к решению задачи защиты данных от изменения. Криптографическая постановка защиты от изменения данных.
21. Защиты от изменения электронных документов (ЭД), её особенности в защите данных от изменения.
22. Обобщённая схема построения аппаратных компонент криптозащиты данных.
23. Защита алгоритма шифрования. Принцип чувствительной области для шифрования. Принцип главного ключа для шифрования.
24. Способы защиты информации на съемных машинных носителях информации. Прозрачный режим шифрования, прозрачный режим шифрования и его реализация на съёмных МНИ.
25. Методы противодействия динамическим и статическим способам снятия защиты про-

грамм от копирования.

26. Понятие ключа в криптографии. Ключевая информация. Роль ключа в криптографической системе.

27. Ключевая информация. Роль ключевой информации в симметричной криптосистеме.

28. Ключевая информация.

29. Охарактеризуйте роль ключевой информации в асимметричной криптосистеме.

30. Роль программной и аппаратной сред в изучении программного обеспечения ПО.

31. Компоненты защищаемой от исследования программы. Инициализатор, секретная часть программы, деструктор (деинициализатор).

32. Функции безопасности направленные на защиту компьютерной программы от трассировки. Защита программы от исследования дизассемблерами.

33. Порядок обратного проектирования программы самими разработчиками, в целях проверки её защищённости от обратного проектирования злоумышленником.

34. Способы защиты компьютерной программы от отладки, как одного из методов обратного проектирования.

35. Понятие итеративности, примеры итеративных подходов применительно к компьютерным технологиям.

36. Определение программного вируса. Вирусы как особый класс разрушающих программных воздействий. «Троянская программа», программная «логическая бомба», программный «червь, программа-вирусоноситель, сетевые вирусы.

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