Атанов Иван Вячеславович
C=RU, S=Ставропольский край, L=Ставрополь, T=Первый проректор, O="ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ "" СТАВРОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ "", СНИЛС=00908046430, ИНН=263507133790, E=glbuh@stgau.ru, G=Иван Вячеславович, SN=Атанов, CN=Атанов Иван Вячеславович
I am the author of this document
your signing location here
2026-03-19 12:46:56

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
СТАВРОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ

Директор/Декан
института экономики, финансов и управления в АПК
Гунько Юлия Александровна
____
____
«___» _____________ 20___ г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ (ОЦЕНОЧНЫХ МАТЕРИАЛОВ)

Б1.В.ДВ.03.02 Информационная безопасность

38.03.01 Экономика

Экономика предприятий и организаций

бакалавр

очная

Ставрополь, 2025

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-1 Сбор, мониторинг и обработка данных для проведения расчетов экономических показателей организации	ПК-1.1 Способен выполнять работы по сбору, обработке и мониторингу исходных данных, необходимых для проведения анализа и планирования показателей производственной, коммерческой и финансово-экономической деятельности организации	**знает** методы по сбору, обработке и мониторингу исходных данных
		умеет проводить работы по сбору, обработке и мониторингу исходных данных
		владеет навыками навыками проведения анализа и планирования показателей производственной, коммерческой и финансово-экономической деятельности организации
ПК-2 Расчет и анализ экономических показателей результатов деятельности организации	ПК-2.1 Обосновывает и применяет статистические, экономико-математические, маркетинговые методы исследования внешней	**знает** статистические, экономико-математические, маркетинговые методы исследования внешней среды и деятельности организации
		умеет применять статистические, экономико-математические, маркетинговые методы исследования внешней среды и деятельности организации, проводить расчеты финансово-экономических показателей, в т.ч. с использованием типовых методик и нормативно-правовых актов

	среды и деятельности организации, проводит расчеты финансово-экономических показателей, в т.ч. с использованием типовых методик и нормативно-правовых актов	**владеет навыками** навыками работы со статистическими, экономико-математическими и маркетинговыми методами исследования вешней среды и деятельности организации

2. Перечень оценочных средств по дисциплине

№	Наименование раздела/темы	Семестр	Код индикаторов достижения компетенций	Оценочное средство проверки результатов достижения индикаторов компетенций
1.	1 раздел. Информационная безопасность			
1.1.	Общая характеристика информационной безопасности	7	ПК-1.1, ПК-2.1	
1.2.	Контрольная точка	7	ПК-1.1, ПК-2.1	Тест
1.3.	Уровни информационной безопасности. Защита информационных ресурсов	7	ПК-1.1, ПК-2.1	
1.4.	Контрольная точка	7	ПК-1.1, ПК-2.1	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	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	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) "Информационная безопасность"

Примерные оценочные материалы для текущего контроля успеваемости

1. Какой характер носит защищаемая информация:
1- смысловой, содержательный характер
2- отличительных признаков
3- ничего не носит
4- цифровую нагрузку

2. Антивирус – программа:
1- удаляющая вирус
2-обнаруживающая и удаляющая вирусы
3- которую устанавливают в файловом контенте
4- созданная в лаборатории Касперский

3. Для чего необходимо запретить сотрудникам использовать компьютерные игры на ПЭВМ, обрабатывающих конфиденциальную информацию:
1-для повышения дисциплины
2-для выполнения своих обязанностей
3-для плана информационной безопасности
4- для уменьшения опасности вирусных атак

4. Защищают и охраняют, как правило информацию:
1- наиболее ценную и важную для ее собственника, ограничение распространения которой приносит ему какую-то пользу или прибыль, возможность эффективно решать стоящие перед ним задачи

2- ограничение распространения которой приносит ему какую-то пользу или прибыль

3- наиболее ценную
4- наиболее важную с возможностью эффективно решать стоящие перед ним задачи.

5. Причинами разрушения могут быть:
1- ошибки программ; аппаратные ошибки; несанкционированные действия; компьютерные вирусы

2- восстановительные мероприятия; ошибки программ; аппаратные ошибки; несанкционированные действия; компьютерные вирусы и др.

3-восстановительные мероприятия; ошибки программ

4- восстановительные мероприятия; несанкционированные действия; компьютерные вирусы

6. Вирус компьютерный – это

1- небольшая, достаточно сложная, тщательно составленная и опасная программа, которая может самостоятельно размножаться, переносить себя на диски, прикрепляться к чужим программам и передаваться по информационным сетям.

2- опасная программа, которая может самостоятельно размножаться, переносить себя на диски, прикрепляться к чужим программам и передаваться по информационным сетям

3- составленная программа, которая может самостоятельно размножаться, переносить себя на диски, прикрепляться к чужим программам и передаваться по информационным сетям

4- небольшая, достаточно сложная, тщательно составленная и опасная программа, которая может самостоятельно размножаться и передаваться по информационным сетям

7 Для чего необходимо периодически проводить проверку контрольным суммированием и применять антивирусные средства

1- для уничтожения вирусных атак

2- для проверки опасности вирусных атак

3- для контроля работы антивируса

4- для уменьшения опасности вирусных атак

8. Массовая информация – информация это:

1- содержащая сообщения информационного характера, подготавливаемая и распространяемая СМИ

2- содержащая сообщения информационного характера, подготавливаемая и распространяемая через Интернет с целью информирования населения

3- содержащая сообщения информационного характера, подготавливаемая и распространяемая СМИ или через Интернет с целью информирования населения

4- содержащая сообщения информационного характера, подготавливаемая и распространяемая с целью информирования населения

9. Официальные документы – документы это:

1- принятые органами законодательной, исполнительной и судебной власти, носящие обязательный информационный характер

2- принятые органами законодательной, исполнительной и судебной власти, носящие обязательный, рекомендательный или информационный характер

3- принятые органами судебной власти, носящие обязательный, рекомендательный или информационный характер

4- принятые органами законодательной, исполнительной, носящие обязательный, рекомендательный или информационный характер

10. Информация, содержащая государственную тайну это:

1– защищаемые государством сведения, создаваемые в условиях секретности в соответствии с законодательством РФ

2– защищаемые государством секреты в соответствии с законодательством РФ

3– защищаемые государством сведения, в соответствии с законодательством РФ

4- сведения, создаваемые в условиях секретности в соответствии с законодательством РФ

11. Информация, составляющая коммерческую тайну это:

1- информация, используемая в экономической деятельности информация, включая ноу-хау

2- научно-техническая, технологическая, коммерческая, организационная или иная используемая в экономической деятельности информация, включая ноу-хау

3- технологическая, коммерческая, организационная или иная используемая в экономической

деятельности информация, включая ноу-хау

4- коммерческая, организационная или иная используемая в экономической деятельности информация, включая ноу-хау

12. Защита информации – это

1- обеспечение информационной безопасности

2- задачи обеспечения информационной безопасности

3- методы и способы обеспечения информационной безопасности

4- комплекс мероприятий, направленных на обеспечение информационной безопасности

13. Статья 23 Конституции РФ гарантирует:

1- Обеспечение конфиденциальности данных.

2- право свободно искать, получать, передавать, производить и распространять информацию.

3-Гарантирует право на личную и семейную тайну, на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений

4- гарантирует право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений

14. Кто является потребителем информации?

1- это пользователь, имеющий доступ к информации.

2- пользователь (потребитель) информации – субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею

3- гражданин РФ в соответствии с законодательством Российской Федерации

4- все, кто допущены согласно списка

15. Закрытый ключ электронной цифровой подписи

1- Закрытый ключ электронной цифровой подписи – уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи

2- Это кодируемая информация специальными кодами.

3- Цифровая последовательность цифрового конструирования.

16. Сколько этапов проектирования физической защиты предприятия?

1- четыре этапа

2- один этап

3- два этапа

4- три этапа

17. Какая должна быть реакция на нарушения режима безопасности:

1- Предотвращение информационного вреда

2- Локализация инцидента и уменьшение наносимого вреда; выявление нарушителя; предупреждение повторных нарушений

3- Прекращение деятельности функционирования источника нарушения

4- Прекращение лицензии

18. Дайте характеристику рисунку:

1- Классификация угроз информационной безопасности
2- Связи информационной безопасности
3- Информационная безопасность и ее отрицательные связи
4- Разделение на классы угроз безопасности

19. Дайте характеристику рисунку:

1- формирование режима информационной безопасности
2- минимизация алгоритмизации информационной безопасности
3- формирование режима ИБ на предприятии
4- алгоритмизация политики информационной безопасности

20. Статья 23 Конституции гарантирует право:

1- на личную и семейную тайну, на тайну переписки и иных сообщений
2- на личную и семейную тайну, на тайну переписки, телефонных переговоров, почтовых иных сообщений
3- на личную и семейную тайну, на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений
4- на личную тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений

21. Статья 29 Конституции гарантирует право:

1- право свободно искать, получать, передавать, производить и распространять информацию любым законным способом
2- право получать, передавать, производить и распространять информацию любым законным способом
3- право свободно искать, производить и распространять информацию любым законным способом
4- право свободно искать, получать, передавать, производить и распространять информацию

22. Уголовный кодекс Российской Федерации статья 272
1- доступ к компьютерной информации по согласованию;
2-неправомерный доступ к компьютерной информации;
3-неправомерный доступ к общей информации;
4- доступ к компьютерной информации;

23. Уголовный кодекс Российской Федерации статья 272
1- создание вредоносных программ для ЭВМ
2 - использование и распространение вредоносных программ для ЭВМ
3- создание, использование вредоносных программ для ЭВМ
4- создание, использование и распространение вредоносных программ для ЭВМ

25. Интересы государства в плане обеспечения конфиденциальности информации нашли наиболее полное выражение в Законе

1- «О государственной тайне"
2- «О государственной и военной тайне"
3- «О конфиденциальности тайны"
4- «О государственной и гражданской тайне"

26. Когда принят Закон "Об информации, информатизации и защите информации"

1- от 23 февраля 1999 года номер 27-ФЗ (принят Государственной Думой 25 января 1995 года)
2-от 20 февраля 2000 года номер 24-ФЗ (принят Государственной Думой 28 января 1995 года)
3- от 20 февраля 1995 года номер 24-ФЗ (принят Государственной Думой 25 января 1995 года)
4- от 26 апреля 1998 года номер 29-ФЗ (принят Государственной Думой 25 января 1995 года)

27. Информация о гражданах (персональные данные) – это

1-сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность;
2-сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие аутентифицировать его личность;
3-сведения о фактах, событиях и обстоятельствах жизни гражданина;
4-сведения об обстоятельствах жизни гражданина, позволяющие идентифицировать его личность;

28. Информационные ресурсы –это:

1- отдельные документы и отдельные массивы документов, документы и массивы документов;
2- отдельные документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах);
3- отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах);
4- отдельные документы и отдельные массивы документов, документы и массивы документов в библиотеках, архивах, фондах, банках данных, других информационных системах;

29. Пользователь (потребитель) информации –это
1- субъект, обращающийся к информационной системе или посреднику за информацией.
2- субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею.
3- пользователь входит в информационную систему и через посредника получает необходимую ему информацию.
4- субъект, обращающийся к посреднику за получением необходимой ему информации и пользующийся ею.

30. Лицензия информационной безопасности – это
1- специальное разрешение на осуществление конкретного вида деятельности при обязательном соблюдении лицензионных требований и условий, выданное лицензирующим органом юридическому лицу или индивидуальному предпринимателю.
2- документ на осуществление конкретного вида деятельности при обязательном соблюдении лицензионных требований и условий, выданное лицензирующим органом юридическому лицу или индивидуальному предпринимателю.
3- удостоверение на осуществление конкретного вида деятельности при обязательном соблюдении лицензионных требований и условий, выданное лицензирующим органом юридическому лицу или индивидуальному предпринимателю.
4- сертификат на осуществление конкретного вида деятельности при обязательном

соблюдении лицензионных требований и условий, выданное лицензирующим органом юридическому лицу или индивидуальному предпринимателю.

31- Основными лицензирующими органами в области защиты информации являются:

1- агентство связи и информации (ФАПСИ) и Гостехкомиссия России.

2- федеральное агентство правительственной связи

3- федеральное агентство правительственной связи и информации (ФАПСИ) и Гостехкомиссия России.

4- Гостехкомиссия России.

32. Электронный документ – это:
1- документ, в котором информация представлена в коде.
2- документ, в котором информация представлена в электронно-цифровой форме.
3- документ, в котором информация представлена в цифре.
4- документ, в котором информация представлена в зашифрованном виде.

33. Сертификат ключа подписи –это:
1- документ с подписью уполномоченного лица удостоверяющего центра
2- документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра
3- документ на бумажном носителе с подписью уполномоченного лица удостоверяющего центра
4- электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра
34. Подтверждение подлинности электронной цифровой подписи в электронном документе это:
1- положительный результат проверки, соответствующей электронной цифровой подписи с использованием ключа подписи
2- результат проверки соответствующим сертифицированным средством электронной цифровой подписи с использованием сертификата ключа подписи
3- положительный результат проверки соответствующим сертифицированным средством
4- положительный результат проверки соответствующим сертифицированным средством электронной цифровой подписи с использованием сертификата ключа подписи

35. Пользователь сертификата ключа подписи –это
1- физическое лицо, использующее полученные в удостоверяющем центре сведения о сертификате ключа подписи для проверки принадлежности электронной цифровой подписи владельцу сертификата ключа подписи
2- лицо, использующее сведения о сертификате ключа подписи для проверки принадлежности электронной цифровой подписи владельцу сертификата ключа подписи
3- физическое лицо, использующее полученные в удостоверяющем центре сведения ключа
4- физическое лицо, использующее полученные в удостоверяющем центре сведения о сертификате ключа подписи для проверки

36. Обеспечение жизненно важных интересов РФ в информационной сфере предполагает достижение:

1- двух основных групп целей
1- трех основных групп целей.
1- четырех основных групп целей.
1- пяти основных групп целей.

37. На процедурном уровне можно выделить сколько класс мер:
1-шесть
2-три
3- пять
4- восемь

38. При проектировании и реализации мер физического управления доступом целесообразно определить:
1- зону ответственности и контролируемую территорию
2- видимую зону и контролируемую территорию
3- периметр безопасности и контролируемую территорию
4- периметр безопасности

39. Оцените рисунок

1- безопасность в информационной системе
2- место угроз безопасности в информационной системе
3- угрозы безопасности
4- информационная система противодействия

40. Формула

1-степень опасности
2- ранжирование
3-фатальность
4- готовность безопасности

41. Дать характеристику рисунку

1- вирусные программы
2- классификация вирусов по алгоритму работы
3- алгоритм работы вирусов
4- совокупность сопряжения вирусных программ

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

Вопросы к зачёту по дисциплине "Информационная безопасность"
1. Что такое информационная безопасность?
2. Какие предпосылки и цели обеспечения информационной безопасности?
3. В чем заключаются национальные интересы РФ в информационной сфере?
4. Что включает в себя информационная борьба?
5. Какие пути решения проблем информационной безопасности РФ существуют?
6. Каковы общие принципы обеспечения защиты информации?
7. Какие имеются виды угроз информационной безопасности предприятия (организации)?
8. Какие источники наиболее распространенных угроз информационной безопасности существуют?
9. Какие виды сетевых атак имеются?
10.Какими способами снизить угрозу сниффинга пакетов?
11.Какие меры по устранению угрозы IP -спуфинга существуют?
12.Что включает борьба с атаками на уровне приложений?
13.Какие существуют проблемы обеспечения безопасности локальных вычислительных сетей?
14.В чем заключается распределенное хранение файлов?
15.Что включают в себя требования по обеспечению комплексной системы информационной безопасности?
16.Какие уровни информационной защиты существуют, их основные составляющие?
17.В чем заключаются задачи криптографии?
18.Зачем нужны ключи?
19.Какая схема шифрования называется многоалфавитной подстановкой?
20.Какие системы шифрования вы знаете?
21.Что включает в себя защита информации от несанкционированного доступа?
22.В чем заключаются достоинства и недостатки программно-аппаратных средств защиты информации?
23.Какие виды механизмов защиты могут быть реализованы для обеспечения идентификации и аутентификации пользователей?
24.Какие задачи выполняет подсистема управления доступом?
25.Какие требования предъявляются к подсистеме протоколирования аудита?
26.Какие виды механизмов защиты могут быть реализованы для обеспечения конфиденциальности данных и сообщений?
27.В чем заключается контроль участников взаимодействия?
28.Какие функции выполняет служба регистрации и наблюдения?
29.Что такое информационно-опасные сигналы, их основные параметры?

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

Перечень тем рефератов:
1. Угрозы информационной безопасности предприятия (организации) и способы борьбы с ними
2. Современные средства защиты информации
3. Современные системы компьютерной безопасности
4. Современные средства противодействия экономическому шпионажу
5. Современные криптографические системы 21
6. Криптоанализ, современное состояние
7. Правовые основы защиты информации
8. Технические аспекты обеспечения защиты информации. Современное состояние
9. Атаки на систему безопасности и современные методы защиты
10. Современные пути решения проблемы информационной безопасности РФ