ЧАСТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
БРЯНСКИЙ ИНСТИТУТ УПРАВЛЕНИЯ И БИЗНЕСА

Фонд
оценочных средств

Информационная безопасность и защита информации

Уровень высшего образования
БАКАЛАВРИАТ

Направление подготовки - 43.03.02 Туризм
Направленность (профиль) – Технология и организация туроператорских и турагентских услуг

Квалификация (степень) выпускника – бакалавр

Форма обучения: очная

Брянск

2025 год

Фонд оценочных средств предназначен для контроля знаний обучающихся по направлению подготовки 43.03.02 Туризм, утвержденным Приказом Министерства образования и науки РФ от 8 июня 2017 г. N 516 «Об утверждении федерального государственного образовательного стандарта высшего образования - бакалавриат по направлению подготовки 43.03.02 Туризм» (с изменениями и дополнениями). Редакция с изменениями N 1456 от 26.11.2020 и Профессиональным стандартом «Экскурсовод (гид)».

Фонд оценочных средств рассмотрен и утвержден на заседании кафедры «Экономики и управления» протокол № 1 от «28» августа 2025 г.

Заведующий кафедрой Экономики и управления — Д.В. Ерохин

Исполнитель: Т.В. Гришанова

Согласовано:

Заведующая секцией Менеджмента — Т.М. Хвостенко

1. **Перечень планируемых результатов обучения, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы УК-8.1; УК-8.2**

Код и описание компетенции	**Код и наименование индикатора достижения УК**	**Планируемые результаты обучения по дисциплине**
УК-8	УК-8. Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов	УК-8.1 Применяет теоретические и практические знания и навыки для обеспечения безопасных условий жизнедеятельности в бытовой и профессиональной сферах
		УК-8.2 Осуществляет оперативные действия по предотвращению чрезвычайных ситуаций и/или их последствий, в том числе при угрозе и возникновении военных конфликтов

ТИПОВЫЕ ИНСТРУКЦИИ ПО ВЫПОЛНЕНИЮ ТЕСТОВЫХ ЗАДАНИЙ

Тип задания	**Инструкция**
Задание закрытого типа с выбором одного или нескольких ответов	**Прочитайте текст и выберите правильный ответ** (Если несколько ответов, то **прочитайте текст и выберите правильные ответы**)
Задание закрытого типа на установление соответствия	**Прочитайте текст и установите соответствие**
Задания закрытого типа на установление правильной последовательности	**Прочитайте текст и установите последовательность**
Задания комбинированного типа с выбором одного верного ответа с обоснованием	**Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа**
Задания комбинированного типа с выбором нескольких ответов с обоснованием	**Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов**
Задания с развернутым ответом	**Прочитайте текст и запишите развернутый обоснованный ответ**

СИСТЕМА ОЦЕНИВАНИЯ ЗАДАНИЙ

Тип задания	Указания по оцениванию	Результат оценивания
Задание закрытого типа на установление соответствия	Задание закрытого типа на установление соответствия считается верным если правильно установлены все соответствия	Верно/неверно
Задания закрытого типа на установление правильной последовательности	Задание закрытого типа на установление правильной последовательности считается верным если правильно указываются все последовательности	Верно/неверно
Задания комбинированного типа с выбором одного верного ответа с обоснованием	Задание комбинированного типа с выбором одного верного ответа из предложенных с обоснованием считается верным если правильно указан ответ и приведены корректные аргументы, используемые при выборе ответа.	Верно/неверно
Задания комбинированного типа с выбором нескольких ответов с обоснованием	Задание комбинированного типа с выбором нескольких ответов из предложенных с обоснованием считается верным если правильно указаны ответы и приведены корректные аргументы, используемые при выборе ответа.	Верно/неверно
Задания открытого типа с развернутым ответом	Задания открытого типа с развернутым ответом считается верным, если ответ совпадает с эталоном по содержанию и полноте.	Верно/неверно

3.Контрольные задания или иные материалы, необходимые для процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения основной профессиональной образовательной программы

3.1. Задания для проведения текущего контроля обучающихся

Содержание вопроса	Компетенции	Уровень освоения
Прочитайте текст и выберите правильный ответ 1. Что такое информационная безопасность? a) Защита компьютера от вирусов. b) Состояние защищенности информации и информационных	УК-8.1; УК-8.2	**Базовый** **1-3 минуты**

систем от всех видов угроз. c) Хранение паролей в безопасном месте. d) Установка антивирусной программы. 2. Основная цель информационной безопасности: a) Полное исключение всех угроз. b) Обеспечение конфиденциальности, целостности и доступности информации. c) Защита только коммерческой тайны. d) Защита только персональных данных. 3. Какие виды угроз информационной безопасности существуют? a) Только вирусы. b) Несанкционированный доступ, несанкционированное разглашение, модификация, разрушение, отказ в обслуживании. c) Только несанкционированный доступ. d) Только несанкционированное разглашение. 4. Что такое конфиденциальность информации? a) Доступность информации для всех. b) Защита информации от несанкционированного доступа. c) Целостность информации. d) Доступность информации для уполномоченных лиц. 5. Что такое целостность информации? a) Защита информации от несанкционированного доступа. b) Защита информации от несанкционированного изменения. c) Доступность информации для всех. d) Доступность информации для уполномоченных лиц. 6. Что такое доступность информации? a) Защита информации от несанкционированного доступа. b) Защита информации от несанкционированного изменения. c) Возможность использования информации уполномоченными лицами в нужный момент времени. d) Хранение информации в безопасном месте. 7. Что такое несанкционированный доступ? a) Доступ к информации с разрешения. b) Доступ к информации без разрешения. c) Доступ к информации в установленное время. d) Доступ к информации в установленном месте. 8. Что такое вирус? a) Полезная программа. b) Злонамеренная программа, способная самостоятельно распространяться.		

c) Системная программа. d) Прикладная программа. 9. Какие виды вирусов существуют? a) Только файловые. b) Файловые, загрузочные, макровирусы, сетевые черви. c) Только сетевые черви. d) Только макровирусы. 10. Что такое антивирусная программа? a) Программа для создания вирусов. b) Программа для обнаружения и удаления вирусов. c) Системная программа. d) Прикладная программа.		
Прочитайте текст и выберите правильный ответ ***Прочитайте текст и выберите правильный ответ*** 11. Что такое фаервол? a) Не имеет значения. b) Программа или аппаратное средство, контролирующее сетевой трафик. c) Только для локальных сетей. d) Только для глобальной сети Интернет. 12. Какие виды фаерволов существуют? a) Только программные. b) Программные, аппаратные. c) Только аппаратные. d) Отсутствуют виды. 13. Что такое шифрование? a) Не имеет значения. b) Преобразование информации в нечитаемый вид. c) Только для текстовых данных. d) Только для графических данных. 14. Какие методы шифрования существуют? a) Только симметричное. b) Симметричное, асимметричное. c) Только асимметричное. d) Отсутствуют методы. 15. Что такое цифровая подпись? a) Не имеет значения. b) Электронная подпись, обеспечивающая аутентификацию и целостность информации. c) Только для электронных документов. d) Только для электронной почты.	УК-8.1; УК-8.2	**Повышенный** **3-5 минут**

16. Что такое доступ к информации? a) Не имеет значения. b) Право на просмотр, использование, изменение и удаление информации. c) Только для уполномоченных лиц. d) Только для владельцев информации. 17. Что такое политика информационной безопасности? a) Не имеет значения. b) Документ, определяющий правила и процедуры обеспечения информационной безопасности. c) Только для коммерческих организаций. d) Только для государственных организаций. 18. Какие разделы должна включать политика информационной безопасности? a) Отсутствуют разделы. b) Цели, принципы, ответственности, процедуры, меры контроля. c) Только цели. d) Только принципы. 19. Что такое контроль доступа? a) Не имеет значения. b) Система мер, регулирующих доступ к информации. c) Только для коммерческой тайны. d) Только для персональных данны x. 20. Какие методы контроля доступа существуют? a) Отсутствуют методы. b) Пароли, смарт-карты, биометрия. c) Только пароли. d) Только смарт-карты.		
Прочитайте текст и запишите развернутый обоснованный ответ Кейс 1: Взлом корпоративной почты Ситуация: В компанию поступила информация о взломе корпоративной почты. Неизвестные получили доступ к переписке сотрудников, включая конфиденциальные данные о проектах и клиентах. Вопрос: Какие действия необходимо предпринять для расследования инцидента и предотвращения подобных ситуаций в будущем?	УК-8.1; УК-8.2	**Высокий** **5-10 минут**

Решение: Необходимо заблокировать доступ к почтовым ящикам, провести расследование с привлечением специалистов по кибербезопасности, изменить все пароли, проанализировать уязвимости системы безопасности, внедрить дополнительные меры защиты (например, многофакторную аутентификацию), информировать сотрудников о правилах информационной безопасности, провести обучение персонала. Кейс 2: Вирусное заражение Ситуация: На компьютерах сотрудников компании обнаружено вредоносное ПО. Часть файлов зашифрована, доступ к ним ограничен. Вопрос: Какие действия необходимо предпринять для устранения угрозы и восстановления доступа к данным? Решение: Необходимо отключить зараженные компьютеры от сети, провести полное сканирование антивирусными программами, удалить вредоносное ПО, восстановить данные из резервных копий (если они есть), обновить антивирусные программы, провести обучение сотрудников правилам информационной безопасности, проанализировать причины заражения и усилить защиту. Кейс 3: Утечка конфиденциальной информации Ситуация: Сотрудник компании передал конфиденциальные данные конкурентам за вознаграждение. Вопрос: Какие меры необходимо предпринять для предотвращения утечек конфиденциальной информации? Решение: Провести расследование, привлечь правоохранительные органы, проанализировать причины утечки, усилить контроль за доступом к конфиденциальной информации, провести обучение сотрудников правилам информационной безопасности, внедрить систему контроля доступа, провести проверку на полиграфе сотрудников с высоким уровнем доступа, пересмотреть политику компании в отношении конфиденциальности. Кейс 4: Отказ в обслуживании (DoS-атака) Ситуация: Веб-сайт компании подвергся DoS-атаке. Доступ к сайту временно ограничен.		

Вопрос: Какие меры необходимо предпринять для защиты от DoS-атак? Решение: Использовать средства защиты от DoS-атак (например, специализированные сервисы или оборудование), усилить защиту сети, провести анализ причин атаки, разработать план реагирования на подобные ситуации, создать резервные серверы.		

3.2.2. Задания для проведения промежуточной аттестации обучающихся

Содержание вопроса	Компетенции	Уровень освоения
Прочитайте текст и выберите правильный ответ 21. Что такое аутентификация? a) Не имеет значения. b) Процесс установления подлинности пользователя или устройства. c) Только для компьютерных систем. d) Только для сетевых систем. 22. Что такое авторизация? a) Не имеет значения. b) Процесс предоставления прав доступа пользователю или устройству. c) Только для компьютерных систем. d) Только для сетевых систем. 23. Что такое учет событий (логгирование)? a) Не имеет значения. b) Запись информации о событиях, происходящих в информационной системе. c) Только для сетевых систем. d) Только для компьютерных систем. 24. Что такое безопасность сетевых технологий? a) Не имеет значения. b) Защита сетевой инфраструктуры от угроз. c) Только для локальных сетей. d) Только для глобальной сети Интернет. 25. Что такое защита от DoS-атак? a) Не имеет значения.	УК-8.1; УК-8.2	**Базовый** **1-3 минуты**

b) Защита от атак отказа в обслуживании. c) Только для сетевых систем. d) Только для компьютерных систем. 26. Что такое VPN? a) Не имеет значения. b) Виртуальная частная сеть. c) Только для коммерческих организаций. d) Только для государственных организаций. 27. Что такое инцидент информационной безопасности? a) Не имеет значения. b) Событие, угрожающее информационной безопасности. c) Только для коммерческих организаций. d) Только для государственных организаций. 28. Что такое реагирование на инциденты? a) Не имеет значения. b) Система мер по предотвращению и ликвидации последствий инцидентов. c) Только для коммерческих организаций. d) Только для государственных организаций. 29. Что такое фишинг? a) Не имеет значения. b) Вид сетевого мошенничества. c) Только для электронной почты. d) Только для социальных сетей. 30. Что такое социальная инженерия? a) Не имеет значения. b) Метод получения конфиденциальной информации путем манипулирования людьми. c) Только для коммерческих организаций. d) Только для государственных организаций		
Прочитайте текст и выберите правильный ответ 31. Что такое шпионское ПО? a) Не имеет значения. b) Программное обеспечение, тайно собирающее информацию. c) Только для коммерческих организаций. d) Только для государственных организаций. 32. Что такое защита от вредоносного кода? a) Не имеет значения. b) Меры по предотвращению попадания и распространения вредоносного кода. c) Только для компьютерных систем. d) Только для сетевых систем.	УК-8.1; УК-8.2	**Повышенный** **3-5 минут**

33. Что такое криптография? a) Не имеет значения. b) Наука о шифровании и расшифровании информации. c) Только для военных целей. d) Только для коммерческих целей. 34. Что такое цифровой сертификат? a) Не имеет значения. b) Электронный документ, подтверждающий подлинность цифровой подписи. c) Только для электронных документов. d) Только для электронной почты. 35. Что такое биометрическая аутентификация? a) Не имеет значения. b) Аутентификация по уникальным биологическим характеристикам. c) Только для государственных организаций. d) Только для коммерческих организаций. 36. Что такое безопасность баз данных? a) Не имеет значения. b) Защита баз данных от несанкционированного доступа и изменения. c) Только для крупных компаний. d) Только для государственных организаций. 37. Что такое безопасность облачных технологий? a) Не имеет значения. b) Защита данных, хранящихся в облаке. c) Только для коммерческих организаций. d) Только для государственных организаций. 38. Что такое управление доступом? a) Не имеет значения. b) Процесс предоставления и отзыва прав доступа к информации. c) Только для компьютерных систем. d) Только для сетевых систем. 39. Что такое безопасность мобильных устройств?		

a) Не имеет значения. b) Защита информации, хранящейся на мобильных устройствах. c) Только для смартфонов. d) Только для планшетов. 40. Что такое анализ уязвимостей? a) Не имеет значения. b) Процесс выявления уязвимостей в информационных системах. c) Только для компьютерных систем.		
Прочитайте текст и запишите развернутый обоснованный ответ Кейс 5: Фишинг Ситуация: Сотрудники компании получили фишинговые письма, маскирующиеся под сообщения от банка. Некоторые сотрудники ввели свои логины и пароли на поддельном сайте. Вопрос: Как защититься от фишинга? Решение: Провести обучение сотрудников правилам информационной безопасности, предупредить о фишинге, ввести политику, запрещающую открытие писем от неизвестных отправителей, использовать многофакторную аутентификацию, предоставить сотрудникам информацию о том, как распознавать фишинговые письма. Кейс 6: Взлом аккаунта в социальной сети Ситуация: Аккаунт компании в социальной сети взломан. Неизвестные разместили на странице некорректную информацию. Вопрос: Как обеспечить безопасность аккаунтов в социальных сетях? Решение: Использовать сложные пароли, включить многофакторную аутентификацию, регулярно обновлять пароли, не использовать один и тот же пароль для разных аккаунтов, не открывать подозрительные ссылки, не переходить по ссылкам из сообщений в соцсетях от неизвестных лиц, настроить приватность аккаунта. Кейс 7: Утеря носителя информации	УК-8.1; УК-8.2	**Высокий** **5-10 минут**

Ситуация: Сотрудник компании потерял флеш-накопитель, на котором хранились конфиденциальные данные. Вопрос: Какие меры необходимо предпринять в случае утери носителя информации? Решение: Немедленно заблокировать доступ к данным на утерянном носителе, проинформировать руководителя о произошедшем, определить уровень значимости утраченных данных, провести расследование, усилить контроль за хранением и использованием носителей информации, предупредить сотрудников об ответственности за утерю данных. Кейс 8: Несанкционированная установка программного обеспечения Ситуация: На компьютерах компании установлено нелицензионное программное обеспечение. Это создает угрозу информационной безопасности. Вопрос: Как обеспечить безопасность использования программного обеспечения? Решение: Использовать только лицензионное ПО, контролировать установку программного обеспечения, создать политику использования ПО, установить систему контроля доступа к установке программ, регулярно обновлять программное обеспечение, проводить обучение сотрудников правилам информационной безопасности.		

3.3. Вопросы к экзамену (промежуточная аттестация), формирование компетенций (УК-8.1; УК-8.2)

1. 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.

4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения основной профессиональной образовательной программы

№ п/п	**Форма контроля/ коды оцениваемых компетенций**	**Процедура оценивания**	**Шкала и критерии оценки, балл**
1.	Экзамен УК-8.1; УК-8.2	Правильность ответов на все вопросы (верное, четкое и достаточно глубокое изложение идей, понятий, фактов и т.д.); Сочетание полноты и лаконичности ответа; Наличие практических навыков по дисциплине (решение задач или заданий); Ориентирование в учебной, научной и специальной литературе; Логика и аргументированность изложения; Грамотное комментирование, приведение примеров, аналогий; Культура ответа.	1. оценка «отлично» - обучающийся должен дать полные, исчерпывающие ответы на вопросы билета, в частности, ответ должен предполагать знание основных понятий и их особенностей, умение правильно определять специфику соответствующих отношений, правильное решение практического задания. Оценка «отлично» предполагает наличие системы знаний по предмету, умение излагать материал в логической последовательности, систематично, грамотным

			языком; 2. оценка «хорошо» - обучающийся должен дать полные ответы на вопросы, указанные в билете. Допускаются неточности при ответе, которые все же не влияют на правильность ответа. Ответ должен предполагать знание основных понятий и их особенностей, умение правильно определять специфику соответствующих отношений. Оценка «хорошо» предполагает наличие системы знаний по предмету, умение излагать материал в логической последовательности, систематично, грамотным языком, однако, допускаются незначительные ошибки, неточности по названным критериям, которые все же не искажают сути соответствующего ответа; 3. оценка «удовлетворительно» - обучающийся должен в целом дать ответы на вопросы, предложенные в билете, ориентироваться в системе дисциплины «Методы психосоциальной коррекции личности», знать основные категории предмета. Оценка «удовлетворительно» предполагает, что материал в основном изложен грамотным языком; оценка «неудовлетворительно» предполагает, что обучающимся либо не дан ответ на вопрос билета, либо обучающийся не знает основных категорий, не может определить предмет дисциплины.
2.	**Тестирование** УК-8.1;	Полнота знаний теоретического контролируемого материала.	**«отлично»** - процент правильных ответов

	УК-8.2	Количество правильных ответов	= > 80%; **«хорошо»** - процент правильных ответов = > 65%; **«удовлетворительно»** - процент правильных ответов = > 50%; **«неудовлетворительно»** - процент правильных ответов < 50%.

С целью определения уровня овладения компетенциями, закрепленными за дисциплиной, в заданные преподавателем сроки проводится текущий и промежуточный контроль знаний, умений и навыков каждого обучающегося. Все виды текущего контроля осуществляются на практических занятиях. Исключение составляет устный опрос, который может проводиться в начале или конце лекции в течение 15-20 мин. с целью закрепления знаний терминологии по дисциплине. При оценке компетенций принимается во внимание формирование профессионального мировоззрения, определенного уровня включённости в занятия, рефлексивные навыки, владение изучаемым материалом.

Процедура оценивания компетенций обучающихся основана на следующих стандартах:

1. Периодичность проведения оценки.

2. Многоступенчатость: оценка (как преподавателем, так и обучающимися группы) и самооценка обучающегося, обсуждение результатов и комплекс мер по устранению недостатков.

3. Единство используемой технологии для всех обучающихся, выполнение условий сопоставимости результатов оценивания.

4. Соблюдение последовательности проведения оценки.

Текущая аттестация обучающихся. Текущая аттестация обучающихся по дисциплине проводится в соответствии с локальными нормативными актами БИУБ и является обязательной.

Текущая аттестация проводится в форме опроса и контрольных мероприятий по оцениванию фактических результатов обучения обучающихся и осуществляется преподавателем дисциплины.

Объектами оценивания выступают:

1) учебная дисциплина (активность на занятиях, своевременность выполнения различных видов заданий, посещаемость всех видов занятий по аттестуемой дисциплине);

2) степень усвоения теоретических знаний в качестве «ключей анализа»;

3) уровень овладения практическими умениями и навыками по всем видам учебной работы;

4) результаты самостоятельной работы (изучение книг из списка основной и дополнительной литературы).

Активность обучающегося на занятиях оценивается на основе выполненных обучающимся работ и заданий, предусмотренных данной рабочей программой дисциплины.

Кроме того, оценивание обучающегося проводится на текущем контроле по дисциплине. Оценивание обучающегося на контрольной неделе проводится преподавателем независимо от наличия или отсутствия обучающегося (по уважительной или неуважительной причине) на занятии. Оценка носит комплексный характер и учитывает достижения обучающегося по основным компонентам учебного процесса за текущий период.

Оценивание обучающегося носит комплексный характер и учитывает достижения обучающегося по основным компонентам учебного процесса за текущий период с выставлением оценок в ведомости.

Промежуточная аттестация обучающихся. Промежуточная аттестация проводится в соответствии с локальными нормативными актами БИУБ и является обязательной.

Промежуточная аттестация проводится в соответствии с учебным планом в виде **экзамена** в период зачётно-экзаменационной сессии в соответствии с графиком проведения.

Обучающиеся допускаются к экзамену в случае выполнения ими учебного плана по дисциплине: выполнения всех заданий и мероприятий, предусмотренных программой дисциплины.

Оценка знаний обучающегося на зачёте определяется его учебными достижениями и результатами текущего контроля знаний и выполнением им заданий.

Основой для определения оценки служит уровень усвоения обучающимися материала, предусмотренного данной рабочей программой дисциплины.

5. Методические указания для обучающихся по освоению дисциплины

Вид деятельности	Методические указания по организации деятельности студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии.
Практические занятия	Проработка рабочей программы, уделяя особое внимание целям и задачам, структуре и содержанию дисциплины. Конспектирование источников. Работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы, работа с текстом. Прослушивание аудио- и видеозаписей по заданной теме, решение расчетно-графических заданий, решение задач по алгоритму и др.
Индивидуальные задания	Знакомство с основной и дополнительной литературой, включая справочные издания, зарубежные источники, конспект основных положений, терминов, сведений, требующихся для запоминания и являющихся основополагающими в этой теме. Составление аннотаций к прочитанным литературным источникам и др.
Самостоятельная работа	Самостоятельная работа проводится с целью: систематизации и закрепления полученных теоретических знаний и практических умений обучающихся; углубления и расширения теоретических знаний студентов; формирования умений использовать нормативную, правовую, справочную документацию, учебную и специальную литературу; развития познавательных способностей и активности обучающихся: творческой инициативы, самостоятельности, ответственности, организованности; формирование самостоятельности мышления, способностей к саморазвитию, совершенствованию и самоорганизации; формирования профессиональных компетенций; развитию исследовательских умений обучающихся. Формы и виды самостоятельной работы: чтение основной и дополнительной литературы

	– самостоятельное изучение материала по рекомендуемым литературным источникам; работа с библиотечным каталогом, самостоятельный подбор необходимой литературы; работа со словарем, справочником; поиск необходимой информации в сети Интернет; конспектирование источников; реферирование источников; составление аннотаций к прочитанным литературным источникам; составление рецензий и отзывов на прочитанный материал; составление обзора публикаций по теме; составление и разработка терминологического словаря; составление хронологической таблицы; составление библиографии (библиографической картотеки); подготовка к различным формам текущей и промежуточной аттестации (к тестированию, зачету, экзамену); выполнение домашних контрольных работ; самостоятельное выполнение практических заданий репродуктивного типа (ответы на вопросы, тесты; выполнение творческих заданий). Технология организации самостоятельной работы обучающихся включает использование информационных и материально-технических ресурсов образовательного учреждения: библиотеку с читальным залом, укомплектованную в соответствии с существующими нормами; учебно-методическую базу учебных кабинетов, лабораторий и зала кодификации; компьютерные классы с возможностью работы в сети Интернет; аудитории (классы) для консультационной деятельности; учебную и учебно-методическую литературу, разработанную с учетом увеличения доли самостоятельной работы студентов, и иные методические материалы. Перед выполнением обучающимися внеаудиторной самостоятельной работы преподаватель проводит консультирование по выполнению задания, который включает цель задания, его содержания, сроки выполнения, ориентировочный объем работы, основные требования к результатам работы, критерии оценки. Во время выполнения обучающимися внеаудиторной самостоятельной работы и при необходимости преподаватель может проводить индивидуальные и групповые консультации. Самостоятельная работа может осуществляться индивидуально или группами обучающихся в зависимости от цели, объема, конкретной тематики самостоятельной работы, уровня сложности, уровня умений обучающихся. Контроль самостоятельной работы предусматривает: ● соотнесение содержания контроля с целями обучения; объективность контроля; ● валидность контроля (соответствие предъявляемых заданий тому, что предполагается проверить); ● дифференциацию контрольно-измерительных материалов. Формы контроля самостоятельной работы: ● просмотр и проверка выполнения самостоятельной работы преподавателем; ● организация самопроверки, ● взаимопроверки выполненного задания в группе; обсуждение

	результатов выполненной работы на занятии; ● проведение письменного опроса; ● проведение устного опроса; ● организация и проведение индивидуального собеседования; организация и проведение собеседования с группой; ● защита отчетов о проделанной работе.
Опрос	Опрос - это средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выявление объема знаний по определенному разделу, теме, проблеме и т.п. Проблематика, выносимая на опрос определена в заданиях для самостоятельной работы обучающегося, а также может определяться преподавателем, ведущим семинарские занятия. Во время проведения опроса обучающийся должен уметь обсудить с преподавателем соответствующую проблематику на уровне диалога.
Коллоквиум	Коллоквиум (от латинского colloquium – разговор, беседа) – одна из форм учебных занятий, беседа преподавателя с учащимися на определенную тему из учебной программы. Цель проведения коллоквиума состоит в выяснении уровня знаний, полученных учащимися в результате прослушивания лекций, посещения семинаров, а также в результате самостоятельного изучения материала. В рамках поставленной цели решаются следующие задачи: ● выяснение качества и степени понимания учащимися лекционного материала; ● развитие и закрепление навыков выражения учащимися своих мыслей; ● расширение вариантов самостоятельной целенаправленной подготовки учащихся; ● развитие навыков обобщения различных литературных источников; ● предоставление возможности учащимся сопоставлять разные точки зрения по рассматриваемому вопросу. В результате проведения коллоквиума преподаватель должен иметь представление: ● качестве лекционного материала; ● сильных и слабых сторонах своей методики чтения лекций; ● сильных и слабых сторонах своей методики проведения семинарских занятий;

	● об уровне самостоятельной работы учащихся; ● об умении обучающихся вести дискуссию и доказывать свою точку зрения; ● степени эрудированности учащихся; ● степени индивидуального освоения материала конкретными обучающимися. В результате проведения коллоквиума обучающийся должен иметь представление: ● об уровне своих знаний по рассматриваемым вопросам в соответствии с требованиями преподавателя и относительно других студентов группы; ● недостатках самостоятельной проработки материала; ● своем умении излагать материал; ● своем умении вести дискуссию и доказывать свою точку зрения. В зависимости от степени подготовки группы можно использовать разные подходы к проведению коллоквиума. В случае, если большинство группы с трудом воспринимает содержание лекций и на практических занятиях демонстрирует недостаточную способность активно оперировать со смысловыми единицами и терминологией курса, то коллоквиум можно разделить на две части. Сначала преподаватель излагает базовые понятия, содержащиеся в программе. Это должно занять не более четверти занятия. Остальные три четверти необходимо посвятить дискуссии, в ходе которой обучающиеся должны убедиться и, главное, убедить друг друга в обоснованности и доказательности полученного видения вопроса и его соответствия реальной практике. Если же преподаватель имеет дело с более подготовленной, самостоятельно думающей и активно усваивающей смысловые единицы и терминологию курса аудиторией, то коллоквиум необходимо провести так, чтобы сами обучающиеся сформулировали изложенные в программе понятия, высказали несовпадающие точки зрения и привели практические примеры. За преподавателем остается роль модератора (ведущего дискуссии), который в конце «лишь» суммирует совместно полученные результаты.
Тестирование	Контроль в виде тестов может использоваться после изучения каждой темы курса. Итоговое тестирование можно проводить в форме: ● компьютерного тестирования, т.е. компьютер произвольно выбирает вопросы из базы данных по степени сложности; ● письменных ответов, т.е. преподаватель задает вопрос и дает несколько вариантов ответа, а обучающийся на отдельном листе записывает номера вопросов и номера соответствующих ответов. Для достижения большей достоверности результатов тестирования

	следует строить текст так, чтобы у обучающихся было не более 40 – 50 секунд для ответа на один вопрос. Итоговый тест должен включать не менее 60 вопросов по всему курсу. Значит, итоговое тестирование займет целое занятие.
Подготовка к экзамену	При подготовке к экзамену необходимо ориентироваться на конспекты лекций, рекомендуемую литературу и др. Основное в подготовке к сдаче экзамена по дисциплине - это повторение всего материала дисциплины, по которому необходимо сдавать экзамен. При подготовке обучающийся весь объем работы должен распределять равномерно по дням, отведенным для подготовки, контролировать каждый день выполнение намеченной работы. Подготовка включает в себя три этапа: ● самостоятельная работа в течение семестра; ● непосредственная подготовка в дни, предшествующие зачёту и экзамену по темам курса; ● подготовка к ответу на задания, содержащиеся в билетах (тестах) экзамена. Для успешной сдачи экзамена по дисциплине «Финансы структур национального хозяйства» обучающиеся должны принимать во внимание, что: ● все основные вопросы, указанные в рабочей программе, нужно знать, понимать их смысл и уметь его разъяснить; ● указанные в рабочей программе формируемые профессиональные компетенции в результате освоения дисциплины должны быть продемонстрированы студентом; ● семинарские занятия способствуют получению более высокого уровня знаний и, как следствие, более высокой оценке на экзамене; готовиться к экзамену необходимо начинать с первой лекции и первого семинара.

ЧАСТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
БРЯНСКИЙ ИНСТИТУТ УПРАВЛЕНИЯ И БИЗНЕСА

КЛЮЧИ ПРАВИЛЬНЫХ ОТВЕТОВ К ФОНДУ ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине: Информационная безопасность и защита информации

Уровень высшего образования
БАКАЛАВРИАТ

Направление подготовки - 43.03.02 Туризм
Направленность (профиль) – Технология и организация туроператорских и турагентских услуг

Квалификация (степень) выпускника – бакалавр

Форма обучения: очная

Брянск

2025 год

ОТВЕТЫ К ТЕСТУ:

Ответы:
1. b
2. b
3. b
4. b
5. b
6. c
7. b
8. b
9. b
10. b
11. b
12. b
13. b
14. b
15. b
16. b
17. b
18. b
19. b
20. b
21. b
22. b
23. b
24. b
25. b
26. b
27. b
28. b
29. b
30. b
31. b
32. b
33. b
34. b
35. b
36. b
37. b
38. b
39. b
40. b

КЕЙСЫ

Кейс 1: Взлом корпоративной почты

Ситуация: В компанию поступила информация о взломе корпоративной почты. Неизвестные получили доступ к переписке сотрудников, включая конфиденциальные данные о проектах и клиентах.
Вопрос: Какие действия необходимо предпринять для расследования инцидента и предотвращения подобных ситуаций в будущем?
Решение: Необходимо заблокировать доступ к почтовым ящикам, провести расследование с привлечением специалистов по кибербезопасности, изменить все пароли, проанализировать уязвимости системы безопасности, внедрить дополнительные меры защиты (например, многофакторную аутентификацию), информировать сотрудников о правилах информационной безопасности, провести обучение персонала.

Кейс 2: Вирусное заражение

Ситуация: На компьютерах сотрудников компании обнаружено вредоносное ПО. Часть файлов зашифрована, доступ к ним ограничен.
Вопрос: Какие действия необходимо предпринять для устранения угрозы и восстановления доступа к данным?
Решение: Необходимо отключить зараженные компьютеры от сети, провести полное сканирование антивирусными программами, удалить вредоносное ПО, восстановить данные из резервных копий (если они есть), обновить антивирусные программы, провести обучение сотрудников правилам информационной безопасности, проанализировать причины заражения и усилить защиту.

Кейс 3: Утечка конфиденциальной информации

Ситуация: Сотрудник компании передал конфиденциальные данные конкурентам за вознаграждение.
Вопрос: Какие меры необходимо предпринять для предотвращения утечек конфиденциальной информации?
Решение: Провести расследование, привлечь правоохранительные органы, проанализировать причины утечки, усилить контроль за доступом к конфиденциальной информации, провести обучение сотрудников правилам информационной безопасности, внедрить систему контроля доступа, провести проверку на полиграфе сотрудников с высоким уровнем доступа, пересмотреть политику компании в отношении конфиденциальности.

Кейс 4: Отказ в обслуживании (DoS-атака)

Ситуация: Веб-сайт компании подвергся DoS-атаке. Доступ к сайту временно ограничен.
Вопрос: Какие меры необходимо предпринять для защиты от DoS-атак?
Решение: Использовать средства защиты от DoS-атак (например, специализированные сервисы или оборудование), усилить защиту сети, провести анализ причин атаки, разработать план реагирования на подобные ситуации, создать резервные серверы.

Кейс 5: Фишинг

Ситуация: Сотрудники компании получили фишинговые письма, маскирующиеся под сообщения от банка. Некоторые сотрудники ввели свои логины и пароли на поддельном сайте.
Вопрос: Как защититься от фишинга?
Решение: Провести обучение сотрудников правилам информационной безопасности, предупредить о фишинге, ввести политику, запрещающую открытие писем от неизвестных отправителей, использовать многофакторную аутентификацию, предоставить сотрудникам информацию о том, как распознавать фишинговые письма.

Кейс 6: Взлом аккаунта в социальной сети
Ситуация: Аккаунт компании в социальной сети взломан. Неизвестные разместили на странице некорректную информацию.
Вопрос: Как обеспечить безопасность аккаунтов в социальных сетях?
Решение: Использовать сложные пароли, включить многофакторную аутентификацию, регулярно обновлять пароли, не использовать один и тот же пароль для разных аккаунтов, не открывать подозрительные ссылки, не переходить по ссылкам из сообщений в соцсетях от неизвестных лиц, настроить приватность аккаунта.

Кейс 7: Утеря носителя информации
Ситуация: Сотрудник компании потерял флеш-накопитель, на котором хранились конфиденциальные данные.
Вопрос: Какие меры необходимо предпринять в случае утери носителя информации?
Решение: Немедленно заблокировать доступ к данным на утерянном носителе, проинформировать руководителя о произошедшем, определить уровень значимости утраченных данных, провести расследование, усилить контроль за хранением и использованием носителей информации, предупредить сотрудников об ответственности за утерю данных.

Кейс 8: Несанкционированная установка программного обеспечения
Ситуация: На компьютерах компании установлено нелицензионное программное обеспечение. Это создает угрозу информационной безопасности.
Вопрос: Как обеспечить безопасность использования программного обеспечения?
Решение: Использовать только лицензионное ПО, контролировать установку программного обеспечения, создать политику использования ПО, установить систему контроля доступа к установке программ, регулярно обновлять программное обеспечение, проводить обучение сотрудников правилам информационной безопасности.