Приложение 7 ОП ВО

Федеральное государственное бюджетное образовательное учреждение высшего образования
«РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»

Факультет «Высшая школа финансов и менеджмента»

Кафедра финансового менеджмента, управленческого учета и международных стандартов финансовой деятельности

УТВЕРЖДЕНА
решением кафедры
Протокол №4 от «11» сентября 2018 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.В.ДВ.03.01 Анализ баз данных и защита информационных систем

направление подготовки (специальность)
38.04.02 «Менеджмент»

направленность (профиль)
«Внутренний контроль и аудит»

Квалификация: магистр

формы обучения: очная

Год набора 2019

Москва, 2018 г.

Автор(ы)–составитель(и):
к.э.н., преподаватель кафедры финансового менеджмента, управленческого учета и международных стандартов финансовой деятельности Блошенко А.А.

Заведующий кафедрой финансового менеджмента, управленческого учета и международных стандартов финансовой деятельности

_____ д.э.н., профессор Е.Н. Лобанова

СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения программы

1.1.Дисциплина Б1.В.ДВ.07.02 «ИТ и ИТ безопасность» обеспечивает овладение следующими компетенциями с учетом этапа:

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ОК-1	Способность к абстрактному мышлению, анализу, синтезу	ОК-1.1	Способность к абстрактному мышлению, анализу первичной информации
ОК-3	Готовность к саморазвитию, самореализации, использованию творческого потенциала	ОК-3.2	Готовность выстраивать траекторию самореализации и использовать творческий потенциал при решении профессиональных задач

1.2. В результате освоения дисциплины у студентов должны быть:

ОТФ/ТФ *(при наличии профстандарта)*/ профессиональные действия	Код этапа освоения компетенции	Результаты обучения
ОТФ - Проведение внутренней аудиторской проверки и (или) выполнение консультационного проекта самостоятельно или в составе группы B/01.7 Проведение внутренней аудиторской проверки самостоятельно или в составе группы	ОК-1.1	на уровне знаний: знание концепций организации управления ИТ, жизненного цикла разработки и запуска систем, базовую ИТ-инфраструктуру, резервное копирование и восстановление данных
		на уровне умений: умение использовать основные элементы ИТ контроля и базовые ИТ контроли при проведении внутреннего аудита
		на уровне навыков: определять риски, ошибки и нарушения в сфере ИТ

ОТФ - Проведение внутренней аудиторской проверки и (или) выполнение консультационного проекта самостоятельно или в составе группы B/01.7 Проведение внутренней аудиторской проверки самостоятельно или в составе группы	ОК-3.2	на уровне знаний: знание основных типов физических средств контроля информационной безопасности
		на уровне умений: умение использовать различные элементы управления информационной безопасности, управлять рисками информационной безопасности
		на уровне навыков: определять и разрабатывать меры, направленные на снижение рисков информационной безопасности

2. Объем и место дисциплины (модуля) в структуре ОП ВО

Дисциплина «Анализ баз данных и защита информационных систем» относится к блоку Б1.В.ДВ. «Дисциплины (модули). Вариативная часть. Дисциплины по выбору». Код дисциплины Б1.В.ДВ.03.02 Дисциплина изучается на 1 курсе, в 2 семестре. Общая трудоемкость дисциплины 72 академических часов (2 ЗЕ) /54 астрономических часов.

Количество академических/астрономических часов, выделяемых на контактную работу с преподавателем составляет 20/15 часов, из них 8/6 – на лекционные занятия, 12/9 – на практические занятия, на самостоятельную работу обучающихся отводится 52/39 часов.

Формой промежуточной аттестации в соответствии с учебным планом является зачет с оценкой.

3. Содержание и структура дисциплины (модуля)

Таблица 2.

№ п/п	Наименование тем (разделов),	Объем дисциплины (модуля), час.						Форма текущего контроля успеваемости**, промежуточной аттестации
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СР	
			Л	ЛР	ПЗ	КСР		
Очная форма обучения								
Тема 1	Аспекты эксплуатации баз данных	38/28,5	4/3		6/4,5		28/21	О
Тема 2	Защита информации в современных информационных системах	34/25,5	4/3		6/4,5		24/18	О, ПРА

Промежуточная аттестация							Зачет с оценкой
Всего:	**72/54**	8/6		12/9		52/39	

Примечание:

** – при применении электронного обучения, дистанционных образовательных технологий в соответствии с учебным планом;*

*** – формы текущего контроля успеваемости: опрос (О), тестирование (Т), контрольная работа (КР), коллоквиум (К), эссе (Э), реферат (Р), диспут (Д), Мини-кейс (МКС), Конкретная ситуация (КС).*

Содержание дисциплины (модуля)

№ п/п	Наименование тем (разделов)	Содержание тем
Тема 1	Аспекты эксплуатации баз данных	Понятие транзакции, ограничения целостности, классификация ограничений целостности. Реализация декларативных ограничений целостности средствами SQL, синтаксис операторов SQL. Восстановление данных, функции восстановления, индивидуальный откат транзакции, восстановление после мягкого/жесткого сбоя. Защита базы данных, основные типы угроз и компьютерные средства контроля, авторизация пользователей, подсхемы, резервное копирование и восстановление, поддержка целостности, шифрование, RAID.
Тема 2	Защита информации в современных информационных системах	Источники, риски и формы атак на компьютерные системы; модели безопасности информационных систем; стандарты безопасности, законодательные меры защиты информации; криптографические модели и методы защиты информации; защита информации в современных информационных системах; защита информации в сети.

4. Методы текущего контроля успеваемости и фонд оценочных средств промежуточной аттестации о дисциплине (модулю)

4.1. Формы и методы текущего контроля успеваемости и промежуточной аттестации.

4.1.1. В ходе реализации дисциплины «Анализ баз данных и защита информационных систем» используются следующие методы текущего контроля успеваемости обучающихся:
– при проведении занятий лекционного типа: опрос (О)
– при проведении занятий семинарского типа: опрос (О), проектно-аналитическое задание (ПРА).

4.1.2. Зачет проводится с применением следующих методов (средств) – в письменной форме (тестирование).

4.2. Материалы текущего контроля успеваемости

Примерный вариант вопросов для опроса к Теме 1.

1. Определите основные виды деятельности в жизненном цикле разработки и запуска системы (определение требований, проектирование, разработка, тестирование, отладка, внедрение, обслуживание и т. д.) и важность изменения контроля на протяжении всего процесса
2. Объясните основные термины базы данных (данные, база данных, запись, объект,

поле, схемы и т. д.) и интернет терминов (HTML и http, URL-адрес, имя домена, браузер, по клику, электронного обмена данными [EDI], cookies и т. д.)
3. Определите основные характеристики программного обеспечения системы (Управление взаимоотношениями с клиентами [CRM] системы; планирование ресурсов предприятия [ERP] системы; управление, риск и комплаенс [GRC] систем и т.д.
4. Объясните базовую ИТ-инфраструктуру и сетевые концепции (сервер, ЭВМ, конфигурацию клиент-сервер, шлюзы, маршрутизаторы, ЛВС, WAN, VPN и т. д.) и выявите потенциальные риски
5. Определите операционные роли сетевого администратора, администратора базы данных и службы поддержки
6. Определите цели и возможное применение концепций организации управления ИТ (COBIT, ISO 27000, ITIL и др.) и основные элементы ИТ контроля
7. Объясните подходы к планированию базы для аварийного восстановления (горячая, теплая, холодная и т. д.)
8. Объясните назначение инструментов резервного копирования данных и систем
9. Объясните назначение процедур восстановления данных и систем

Примерный вариант вопросов для опроса к Теме 2.

1. Определите типы распространенных физических средств контроля безопасности (карты, ключи, биометрия и др.).)
2. Определите различные формы аутентификации пользователей и контроля авторизации (пароль, два уровня аутентификации, биометрические, цифровые подписи и т. д.) и выявите потенциальные риски
3. Объясните назначение и использование различных элементов управления информационной безопасностью (шифрование, брэндмауэры, антивирусы и т. д.)
4. Опишите законы о конфиденциальности данных и их потенциальное влияние на политику и практику обеспечения безопасности данных.
5. Расскажите о новых технологиях и их влиянии на безопасность ("принеси свое устройство" [byod], смартустройств, интернета вещей [IoT] и т. д.)
6. Существующие и возникающие риски информационной безопасности (взлом, пиратство, подделка, вымогателей атак, фишинг-атак и др.)
7. Опишите политику кибербезопасности и информационной безопасности.

Примерный вариант Проектно-аналитического задания к Теме 2.

1. Разработать программу предупреждения и противодействия нарушениям ИТ безопасности (политику кибербезопасности и информационной безопасности).
2. Разработать базовые ИТ контроли для не менее чем 10 рискам информационной безопасности.
3. Разработать рекомендации по созданию эффективной ИТ-инфраструктуры.
4. Разработать рекомендации по созданию эффективной ролевой модели, аутентификации пользователей и контроля авторизации.
5. Разработать требования к защите конфиденциальных данных и модель внедрения режима конфиденциальности.

4.3.Оценочные средства для промежуточной аттестации обучающихся.

4.3.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы. Показатели и критерии оценивания компетенций с учетом этапа их формирования

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ОК-1	Способность к абстрактному мышлению, анализу, синтезу	ОК-1.1	Способность к абстрактному мышлению, анализу первичной информации
ОК-3	Готовность к саморазвитию, самореализации, использованию творческого потенциала	ОК-3.2	Готовность выстраивать траекторию самореализации и использовать творческий потенциал при решении профессиональных задач

Этап освоения компетенции	**Показатель оценивания** *Что делает обучающийся (какие действия способен выполнить), подтверждая этап освоения компетенции*	**Критерий оценивания** *Как (с каким качеством) выполняется действие. Соответствует оценке «отлично» в шкале оценивания в РПД.*
ОК-1.1 Способность к абстрактному мышлению, анализу первичной информации	Знает жизненный цикл разработки и запуска информационных систем, термины баз данных, концепции организации управления ИТ. Способен сформулировать базовые ИТ контроли. Способен оценить эффективность ИТ-инфраструктуры, систем резервного копирования и восстановления данных.	Демонстрирует знания жизненного цикла разработки и запуска информационных систем, терминов баз данных, концепции организации управления ИТ. Разрабатывает и дает оценку эффективности базовых ИТ контролей. Дает оценку эффективности ИТ-инфраструктуры, систем резервного копирования и восстановления данных.

Этап освоения компетенции	Показатель оценивания *Что делает обучающийся (какие действия способен выполнить), подтверждая этап освоения компетенции*	Критерий оценивания *Как (с каким качеством) выполняется действие. Соответствует оценке «отлично» в шкале оценивания в РПД.*
ОК-3.2 Готовность выстраивать траекторию самореализации и использовать творческий потенциал при решении профессиональных задач	Знает основные типы физических средств контроля информационной безопасности, принципы формирования политики кибербезопасности и информационной безопасности, требования к защите конфиденциальных данных, к ролевой модели, аутентификации пользователей и контроля авторизации. Способен использовать различные элементы управления информационной безопасностью, управлять рисками информационной безопасности. Способен разрабатывать меры, направленные на снижение рисков информационной безопасности.	Демонстрирует знания основных типов физических средств контроля информационной безопасности, принципов формирования политики кибербезопасности и информационной безопасности, требований к защите конфиденциальных данных, к ролевой модели, аутентификации пользователей и контроля авторизации. При проведении внутреннего аудита дает оценку эффективности использования элементов информационной безопасности и управления рисками информационной безопасности. При формировании аудиторских рекомендаций разрабатывает меры, направленные на снижение рисков информационной безопасности.

4.3.2. Типовые оценочные средства

Список вопросов для подготовки к зачету с оценкой:

1. **Как называется умышленно искаженная информация?**

+ Дезинформация
- Информативный поток
- Достоверная информация
- Перестает быть информацией

2. **Как называется информация, к которой ограничен доступ?**

+ Конфиденциальная
- Противозаконная
- Открытая

- Недоступная

3. **Какими путями может быть получена информация?**

+ проведением, покупкой и противоправным добыванием информации научных исследований
- захватом и взломом ПК информации научных исследований
- добыванием информации из внешних источников и скремблированием информации научных исследовании
- захватом и взломом защитной системы для информации научных исследований

4. **Как называются компьютерные системы, в которых обеспечивается безопасность информации?**

+ защищенные КС
- небезопасные КС
- Само достаточные КС
- Саморегулирующиеся КС

5. **Основной документ, на основе которого проводится политика информационной безопасности?**

+ программа информационной безопасности
- регламент информационной безопасности
- политическая информационная безопасность
- Протекторат

6. **В зависимости от формы представления информация может быть разделена на?**

+ Речевую, документированную и телекоммуникационную
- Мысль, слово и речь
- цифровая, звуковая и тайная
- цифровая, звуковая

7. **К каким процессам относят процессы сбора, обработки, накопления, хранения, поиска и распространения информации**

+ Информационным процессам
- Мыслительным процессам
- Машинным процессам
- Микропроцессам

8. **Что называют защитой информации?**

+ Все ответы верны
- Называют деятельность по предотвращению утечки защищаемой информации
- Называют деятельность по предотвращению несанкционированных воздействий на защищаемую информацию
- Называют деятельность по предотвращению непреднамеренных воздействий на защищаемую информацию

9. **Под непреднамеренным воздействием на защищаемую информацию понимают?**

+ Воздействие на нее из-за ошибок пользователя, сбоя технических или программных средств и воздействие природных явлений
- Процесс ее преобразования, при котором содержание информации изменяется на ложную
- Возможности ее преобразования, при котором содержание информации изменяется на ложную информацию

- Не ограничения доступа в отдельные отрасли экономики или на конкретные производства

10. Шифрование информации это

+ Процесс ее преобразования, при котором содержание информации становится непонятным для не обладающих соответствующими полномочиями субъектов
- Процесс преобразования, при котором информация удаляется
- Процесс ее преобразования, при котором содержание информации изменяется на ложную
- Процесс преобразования информации в машинный код

11. Основные предметные направления защиты информации?

+ охрана государственной, коммерческой, служебной, банковской тайн, персональных данных и интеллектуальной собственности
- Охрана золотого фонда страны
- Определение ценности информации
- Усовершенствование скорости передачи информации

12. Государственная тайна это

+ защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности страны
- ограничения доступа в отдельные отрасли экономики или на конкретные производства
- защищаемые банками и иными кредитными организациями сведения о банковских операциях
- защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей

13. Коммерческая тайна это….

- защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности страны
+ ограничения доступа в отдельные отрасли экономики или на конкретные производства
- защищаемые банками и иными кредитными организациями сведения о банковских операциях
- защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей

14. Банковская тайна это….

- защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности страны
- ограничения доступа в отдельные отрасли экономики или на конкретные производства
+ защищаемые банками и иными кредитными организациями сведения о банковских операциях
- защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей

15. Профессиональная тайна

- защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности страны
- ограничения доступа в отдельные отрасли экономики или на конкретные производства
- защищаемые банками и иными кредитными организациями сведения о банковских операциях

+ защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей

16. Как называется тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений?

+ Тайна связи
- Нотариальная тайна
- Адвокатская тайна
- Тайна страхования

17. Элемент аппаратной защиты, где используется установка источников бесперебойного питания (UPS)?

+ защита от сбоев в электропитании
- защита от сбоев серверов, рабочих станций и локальных компьютеров
- защита от сбоев устройств для хранения информации
- защита от утечек информации электромагнитных излучений

18. Функция защиты информационной системы, гарантирующая то, что доступ к информации, хранящейся в системе может быть осуществлен только тем лицам, которые на это имеют право

- управление доступом
+ конфиденциальность
- аутентичность
- целостность
- доступность

19. Элемент аппаратной защиты, где используется резервирование особо важных компьютерных подсистем

- защита от сбоев в электропитании
+ защита от сбоев серверов, рабочих станций и локальных компьютеров
- защита от сбоев устройств для хранения информации
- защита от утечек информации электромагнитных излучений

20. Элемент аппаратной защиты, где используется организация надежной и эффективной системы резервного копирования и дублирования данных

- защита от сбоев в электропитании
- защита от сбоев серверов, рабочих станций и локальных компьютеров
+ защита от сбоев устройств для хранения информации
- защита от утечек информации электромагнитных излучений

21. Элемент аппаратной защиты, где используется экранирование, фильтрацию, заземление, электромагнитное зашумление, а также средства ослабления уровней нежелательных электромагнитных излучений.

- защита от сбоев в электропитании
- защита от сбоев серверов, рабочих станций и локальных компьютеров
- защита от сбоев устройств для хранения информации
+ защита от утечек информации электромагнитных излучений

22. Какая из перечисленных атак на поток информации является пассивной:

+ перехват.
- имитация.
- модификация.
- фальсификация.

- прерывание.

23. К открытым источникам информация относятся.

+ Газеты, Радио, Новости
- Информация украденная у спецслужб
- Из вскрытого сейфа
- Украденная из правительственной организации

24. Технические каналы утечки информации делятся на…

+ Все перечисленное
- Акустические и виброакустические
- Электрические
- Оптические

25. Какой технический канал утечки отвечает за распространение звуковых колебаний в любом звукопроводящем материале или среде?

+ Акустические и виброакустические
- Электрические
- Оптические
- Радиоканалы

26. Какой технический канал утечки отвечает за напряжение и токи в различных токопроводящих коммуникациях?

- Акустические и виброакустические
+ Электрические
- Оптические
- Радиоканалы

27. Какой технический канал утечки отвечает за электромагнитные излучения радиодиапазона?

- Акустические и виброакустические
- Электрические
- Оптические
+ Радиоканалы

28. Какой технический канал утечки отвечает за электромагнитные излучения в видимой, инфракрасной и ультрафиолетовой частях спектра?

- Акустические и виброакустические
- Электрические
+ Оптические
- Радиоканалы

29. По сведениям Media и Pricewaterhouse Coopers, на чью долю приходится 60% всех инцидентов IT-безопасности?

- Хакерские атаки
- Различные незаконные проникновения
+ Инсайдеры
- Технические компании

30. Учет всех возможных коммуникационных каналов, обеспечения физической безопасности, шифрования резервных копий и информации, покидающей корпоративный периметр, и других организационных мероприятий это?

- Индивидуальный подход к защите

+ Комплексный подход к защите
- Смешанный подход к защите
- Рациональный подход к защите

31. Меры по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе

+ Информационная безопасность
- Защитные технологии
- Заземление
- Конфиденциальность

32. Можно выделить следующие направления мер информационной безопасности

- Правовые
- Организационные
+ Все ответы верны
- Технические

33. Что можно отнести к правовым мерам ИБ?

+ Разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства
- охрану вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра итд
- Защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем, организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев, установку оборудования обнаружения и тушения пожара, оборудования обнаружения воды, принятие конструкционных мер защиты от хищений, саботажа, диверсий, взрывов, установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и многое другое
- охрану вычислительного центра, установку сигнализации и многое другое

34. Что можно отнести к организационным мерам ИБ?

- Разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства.
+ Охрану вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра и т.д.
- Защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем.
- Охрану работоспособности отдельных звеньев и организацию вычислительных сетей с возможностью перераспределения ресурсов.
- Принятие конструкционных мер защиты от хищений, саботажа, диверсий, взрывов, установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и многое другое.

35. Что можно отнести к техническим мерам ИБ?

- Разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства

- Охрану вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра и т.д.
+ Защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем, организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев и многое другое
- Простые и доступные меры защиты от хищений, саботажа, диверсий, взрывов
- В административных местах установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и многое другое.

Итоговая шкала оценивания по дисциплине

Критерии оценки	**Оценка (баллы)**
Выполнены все задания теста (не менее чем на 70% верно). Продемонстрированы знания прикладного и системного программного обеспечения, схем организации ИТ-инфраструктуры, аварийного восстановления. Продемонстрировано понимание контроля информационных технологий и информационной безопасности.	Зачтено – 70-100 баллов
Выполнено менее 70% заданий теста. Не продемонстрированы знания прикладного и системного программного обеспечения, схем организации ИТ-инфраструктуры, аварийного восстановления. Не продемонстрировано понимание контроля информационных технологий и информационной безопасности.	Не зачтено – 0-69 баллов

4.4. Методические материалы

Промежуточная аттестация (зачет) по дисциплине «Анализ баз данных и защита информационных систем» проходит в форме тестирования. Студенты одновременно решают тестовые задания. Каждый студент получает свой персональный вариант теста. На организационную подготовку отводится от 20 до 30 минут, на написание теста – 90 минут. Во время организационной подготовки студентам разъясняются правила проведения зачета и выдаются маркированные листы для ответов и заполнения. По истечении отведенного времени обучающийся докладывает экзаменатору о готовности и сдает тестовое задание на проверку. Экзаменатор может задавать обучающемуся дополнительные и уточняющие вопросы в пределах учебного материала, вынесенного на зачет.
Результат по сдаче зачета объявляется студентам, вносится в экзаменационную ведомость и в зачетную книжку. Оценка «не зачтено» проставляется только в ведомости.

5. Методические указания для обучающихся по освоению дисциплины (модуля)

Методические рекомендации по оцениванию тестирования

Тестирование является одним из самых объективных и простых способом контроля успеваемости. Будучи формализованной и стандартизированной формой проверки не вызывает трудности при проведении и позволяет быстро получить результат. Студентам выдается тест с инструкцией следующего содержания.

В каждом вопросе теста выберите правильный ответ и отметьте его крестиком в форме для ответов, а в самом тексте теста правильный ответ обведите кружком.
Рекомендуется использование обычного калькулятора.
Если в вопросе не сказано иное, то округление выполняйте до 2-х знаков после запятой по обычным правилам арифметики.
Текст теста у вас остается для разбора, а подписанную форму для ответов (Ф.И.О. полностью) вы сдаете преподавателю.
По окончании тестирования преподаватель подводит итоги опроса и выставляет соответствующие баллы.

Методические рекомендации по оцениванию проектно-аналитического задания (ПРА)

ПРА выполняется индивидуально Результаты оформляются в виде письменного отчета, включающего описание цели и задач работы, круг рассматриваемых проблем и методы их решения, результаты анализа используемого материала, их интерпретация и общие выводы.

При оценивании ПРА учитывается умение логически обрабатывать, сравнивать, сопоставлять и обобщать, классифицировать материал по тем или иным признакам, высказывать свое отношение к описываемым явлениям, событиям и давать собственную оценку.

Требования к организации самостоятельной работы студентов при подготовке к аудиторным занятиям

1. Подготовка к лекциям

Главное в период подготовки к лекционным занятиям – научиться методам самостоятельного умственного труда, сознательно развивать свои творческие способности и овладевать навыками творческой работы. Для этого необходимо строго соблюдать дисциплину учебы и поведения. Четкое планирование своего рабочего времени и отдыха является необходимым условием для успешной самостоятельной работы. В основу его нужно положить рабочие программы изучаемых в семестре дисциплин. Ежедневной учебной работе студенту следует уделять 9–10 часов своего времени, т.е. при шести часах аудиторных занятий самостоятельной работе необходимо отводить 3–4 часа. Каждому студенту следует составлять еженедельный и семестровый планы работы, а также план на каждый рабочий день. С вечера всегда надо распределять работу на завтрашний день. В конце каждого дня целесообразно подводить итог работы: тщательно проверить, все ли выполнено по намеченному плану, не было ли каких-либо отступлений, а если были, по какой причине это произошло. Нужно осуществлять самоконтроль, который является необходимым условием успешной учебы. Если что-то осталось невыполненным, необходимо изыскать время для завершения этой части работы, не уменьшая объема недельного плана.

2. Самостоятельная работа на лекции

Слушание и запись лекций – сложный вид вузовской аудиторной работы. Внимательное слушание и конспектирование лекций предполагает интенсивную умственную деятельность студента. Краткие записи лекций, их конспектирование помогает усвоить учебный материал. Конспект является полезным тогда, когда записано самое существенное, основное и сделано это самим студентом. Не надо стремиться записать дословно всю

лекцию. Такое «конспектирование» приносит больше вреда, чем пользы. Запись лекций рекомендуется вести по возможности собственными формулировками. Желательно запись осуществлять на одной странице, а следующую оставлять для проработки учебного материала самостоятельно в домашних условиях. Конспект лекции лучше подразделять на пункты, параграфы, соблюдая красную строку. Этому в большой степени будут способствовать пункты плана лекции, предложенные преподавателям. Принципиальные места, определения, формулы и другое следует сопровождать замечаниями «важно», «особо важно», «хорошо запомнить» и т.п. Можно делать это и с помощью разноцветных маркеров или ручек. Лучше если они будут собственными, чтобы не приходилось просить их у однокурсников и тем самым не отвлекать их во время лекции. Целесообразно разработать собственную «маркографию» (значки, символы), сокращения слов. Не лишним будет и изучение основ стенографии. Работая над конспектом лекций, всегда необходимо использовать не только учебник, но и ту литературу, которую дополнительно рекомендовал лектор. Именно такая серьезная, кропотливая работа с лекционным материалом позволит глубоко овладеть знаниями.

3. Подготовка к семинарским занятиям

Подготовку к каждому семинарскому занятию каждый студент должен начать с ознакомления с планом семинарского занятия, который отражает содержание предложенной темы. Тщательное продумывание и изучение вопросов плана основывается на проработке текущего материала лекции, а затем изучения обязательной и дополнительной литературы, рекомендованную к данной теме. На основе индивидуальных предпочтений студенту необходимо самостоятельно выбрать тему доклада по проблеме семинара и по возможности подготовить по нему презентацию. Если программой дисциплины предусмотрено выполнение практического задания, то его необходимо выполнить с учетом предложенной инструкции (устно или 10 письменно). Все новые понятия по изучаемой теме необходимо выучить наизусть и внести в глоссарий, который целесообразно вести с самого начала изучения курса. Результат такой работы должен проявиться в способности студента свободно ответить на теоретические вопросы семинара, его выступлении и участии в коллективном обсуждении вопросов изучаемой темы, правильном выполнении практических заданий и контрольных работ. Структура семинара
В зависимости от содержания и количества отведенного времени на изучение каждой темы семинарское занятие может состоять из четырех-пяти частей:
1. Обсуждение теоретических вопросов, определенных программой дисциплины.
2. Доклад и/ или выступление с презентациями по проблеме семинара.
3. Обсуждение выступлений по теме – дискуссия.
4. Выполнение практического задания с последующим разбором полученных результатов или обсуждение практического задания, выполненного дома, если это предусмотрено программой.
5. Подведение итогов занятия.
Первая часть – обсуждение теоретических вопросов - проводится в виде фронтальной беседы со всей группой и включает выборочную проверку преподавателем теоретических знаний студентов. Примерная продолжительность — до 15 минут. Вторая часть — выступление студентов с докладами, которые должны сопровождаться презентациями с целью усиления наглядности восприятия, по одному из вопросов семинарского занятия. Обязательный элемент доклада – представление и анализ статистических данных, обоснование социальных последствий любого экономического факта, явления или процесса. Примерная продолжительность — 20-25 минут. После докладов следует их обсуждение – дискуссия. В ходе этого этапа семинарского занятия могут быть заданы уточняющие вопросы к докладчикам. Примерная продолжительность – до 15-20 минут. Если программой предусмотрено выполнение практического задания в рамках конкретной

темы, то преподавателями определяется его содержание и дается время на его выполнение, а замет идет обсуждение результатов. Если практическое задание должно было быть выполнено дома, то на семинарском занятии преподаватель проверяет его выполнение (устно или письменно). Примерная продолжительность – 15-20 минут. Подведением итогов заканчивается семинарское занятие. Студентам должны быть объявлены оценки за работу и даны их четкие обоснования. Примерная продолжительность — 5 минут.

4. Работа с литературными источниками

В процессе подготовки к семинарским занятиям, студентам необходимо обратить особое внимание на самостоятельное изучение рекомендованной учебно-методической (а также научной и популярной) литературы. Самостоятельная работа с учебниками, учебными пособиями, научной, справочной и популярной литературой, материалами периодических изданий и Интернета, статистическими данными является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у студентов свое отношение к конкретной проблеме. Более глубокому раскрытию вопросов способствует знакомство с дополнительной литературой, рекомендованной преподавателем по каждой теме семинарского или практического занятия, что позволяет студентам проявить свою индивидуальность в рамках выступления на данных занятиях, выявить широкий спектр мнений по изучаемой проблеме.

6. Учебная литература и ресурсы информационно-телекоммуникационной сети "Интернет", включая перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

6.1. Основная литература:

1. Джеймс Л. Фишинг. Техника компьютерных преступлений. 2008. М. изд. НТ Пресс;
2. Ю. Родичев «Нормативная база и стандарты в области информационной безопасности». 2017. изд. Питер;
3. А. Бабаш, Е. Баранова, Д. Ларин «Информационная безопасность. История защиты информации в России». 2015. изд. КДУ;
4. Е. Баранова, А. Бабаш «Информационная безопасность и защита информации» 3-е изд. 2016. Изд. РИОР, Инфра-М;
5. В. Бондарев «Введение в информационную безопасность автоматизированных систем». 2016. изд. МГТУ им. Н. Э. Баумана;
6. С. Нестеров «Основы информационной безопасности». 2016. изд. Лань;
7. А. Бирюков «Информационная безопасность: защита и нападение» 2-е изд. 2017. изд. ДМК Пресс.

6.2. Дополнительная литература:

8. Жуков Ю.В. Основы веб-хакинга: нападение и защита. 2011. М.-СПб. Изд. «Питер»;
9. Лапонина О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия. 2011. М. изд. «БИНОМ»;
10. Меньшаков Ю.К. Теоретические основы технических разведок. 2008. М. изд. МГТУ им. Н.Э. Баумана;
11. Меньшаков Ю.К. Виды и средства иностранных технических разведок. 2009. М.

изд. МГТУ им. Н.Э. Баумана;
12. Меньшаков Ю.К. Основы защиты от технических разведок. 2011. М. изд. МГТУ им. Н.Э. Баумана;
13. Просис К., Мандиа К. Расследование компьютерных преступлений. 2012. М. изд. «Лори»;

6.3. Перечень нормативно-правовых актов Российской Федерации:

1. Федеральный закон «О персональных данных»;
2. Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и защите информации»;
3. Федеральный закон «Об электронной подписи»;
4. ГОСТ Р ИСО/МЭК 20000 «Информационная технология. Менеджмент услуг»;
5. ГОСТ Р 51898-2002, «Аспекты безопасности. Правила включения в стандарты»;
6. ГОСТ Р ИСО/МЭК 13335-1-2006, «Информационная технология. Методы и средства обеспечения безопасности»;
7. СТО БР ИББС-1.0-2008 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения».
8. Аудит информационной безопасности в российских банках, Стандарт Банка России СТО БР ИББС-1.1-2007 (Распоряжение Банка России от 28.04.2007 N Р-345)

6.4. Интернет-ресурсы:

www.prmia.org – Международная ассоциация риск-менеджеров (PRMIA)

https://www.axelos.com/best-practice-solutions/itil - IT Infrastructure Library — библиотека инфраструктуры информационных технологий

https://www.isaca.org/pages/default.aspx - ISACA - международная Ассоциация аудита и контроля информационных систем

https://engage.isaca.org/moscow/home - Московское отделение ISACA

http://www.isaca.org/knowledge-center/cobit/Pages/Overview.aspx - COBIT (сокращение от англ. Control Objectives for Information and Related Technologies — «Задачи управления для информационных и смежных технологий») — методология управления информационными технологиями, принадлежащая и разрабатываемая некоммерческой организацией ISACA

7.Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

Занятия проводятся в учебных аудиториях, оснащенных рабочим местом преподавателя (стол, стул, кафедра), рабочими местами студентов (столы, стулья) по количеству студентов, доской меловой или белой для написания маркерами или флипчартом для бумаги большого формата, маркерами (красный, черный, зеленый, синий), губкой для досок, оборудованием для показа презентаций и слайдов (компьютер, проектор, экран).

Используется следующее программное обеспечение:

Microsoft Windows 10 LTSB 1607
Количество 2607
Правообладатель Microsoft Corporation
Дата покупки / продления06.12.2016
Контракт59/07-16/0373100037616000052-0008121-03
Продавец ООО «ЛАНИТ-Интеграция»
Покупатель РАНХиГС
Дата окончания 31.12.2017
Срок подписки 1 год / 3 года

Microsoft Office Professional 2016
Количество 2607
Правообладатель Microsoft Corporation
Дата покупки / продления 06.12.2016
Контракт59/07-16/0373100037616000052-0008121-03
Продавец ООО «ЛАНИТ-Интеграция»
Покупатель РАНХиГС
Дата окончания 31.12.2017
Срок подписки 1 год / 3 года

Acrobat Professional AcademicEdition License Russian
Multiple Platforms (Adobe, 65258631AE01A00)
Количество 50
Правообладатель Adobe
Дата покупки / продления 03.04.2017
Контракт #15/08-17
Продавец SoftLine
Покупатель РАНХиГС
Дата окончания 03.04.2018