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

Факультет «Институт менеджмента и маркетинга»
(наименование структурного подразделения (института/факультета)
кафедра «Финансы и страхование»
(наименование кафедры)

УТВЕРЖДЕН

решением *Ученого совета факультета «Институт менеджмента и маркетинга»*

Протокол от «28» августа 2017г.

№ 3

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ДВ.03.02 Информационная безопасность
(индекс, наименование дисциплины (модуля), в соответствии с учебным планом)

38.03.01 Экономика
(код, наименование направления подготовки)

Экономика в топливно-энергетическом комплексе
(направленность (профиль))

Бакалавр
(квалификация)

очная
(форма обучения)

Год набора - 2018

Москва, 2017 г.

Автор(ы)–составитель(и):

канд.техн.наук,доцент,доцент_____А.В.Панов
(ученая степень и(или) ученое звание, должность) (наименование кафедры) (Ф.И.О.)

Заведующий кафедрой:

Зав. кафедрой «Финансы и страхование»___доктор экон.наук____ А.С.Миллерман
(наименование кафедры) (ученая степень и(или) ученое звание) (Ф.И.О.)

СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения программы....4
2. Объем и место дисциплины (модуля) в структуре ОП ВО....4
3. Содержание и структура дисциплины (модуля)....5
4. Материалы текущего контроля успеваемости обучающихся и....6
фонд оценочных средств промежуточной аттестации по дисциплине....6
5. Методические указания для обучающихся по освоению дисциплины....10
6. Учебная литература и ресурсы информационно-телекоммуникационной сети "Интернет", включая перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)....11
6.1. Основная литература....11
6.2. Дополнительная литература....11
6.3. Учебно-методическое обеспечение самостоятельной работы....11
6.4. Нормативные правовые документы....11
6.5. Интернет-ресурсы....11
6.6. Иные источники....11
7. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы....12

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

1.1. Дисциплина Б1.В.ДВ.03.02 Информационная безопасность обеспечивает овладение следующей компетенцией:

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ОПК-1	способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-1.3	Готовность разрабатывать проекты решений по улучшению системы информационной безопасности в соответствии с существующей практикой с учетом результатов аналитической работы. Формирование навыков и развитие навыков прогнозирования и защиты бизнеса от внутренних и внешних вызовов

1.2. В результате освоения дисциплины у студентов должны быть сформированы:

Код этапа освоения компетенции	Результаты обучения
ОПК-1.3	на уровне знаний: основы системы информационной и библиографической культуры; основы информационно-коммуникационных технологий; основные требования информационной безопасности при решении задач профессиональной деятельности; специфику различных требований, предъявляемых к информационной безопасности
	на уровне умений: анализировать библиографический и информационный материал используя информационно-коммуникационные технологии; определять стандартные задачи профессиональной деятельности с учетом основных требований информационной безопасности.
	на уровне навыков: навыками анализа профессионально-практической деятельности работы с использованием основных требований информационной безопасности с применением информационно-коммуникационных технологий

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

Объем дисциплины

Общая трудоемкость дисциплины – 3 з.е.

54 часа выделены на контактную работу с преподавателем и 54 часа на

самостоятельную работу обучающихся.

Место дисциплины в структуре ОП ВО

Дисциплина Б1.В.ДВ.03.02 Информационная безопасность изучается на 3 курсе в 6 семестре.

Дисциплина Информационная безопасность базируется на знаниях, полученных в рамках следующих дисциплин: Микроэкономика; Макроэкономика; Финансы; Деньги, кредит, банки. Знания, полученные в курсе Информационная безопасность, используются студентами при выполнении выпускных квалификационных работ и в дальнейшей практической работе.

Форма промежуточной аттестации – зачет с оценкой.

3. Содержание и структура дисциплины (модуля)

Очная форма обучения

№ 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	Введение в информационную безопасность	11	1	-	-	1	9	Н
Тема 2	Правовое обеспечение информационной безопасности	18	2	-	6	1	9	О
Тема 3	Организационное обеспечение информационной безопасности	19	3	-	6	1	9	О
Тема 4	Технические средства и методы защиты информации	19	3	-	6	1	9	О
Тема 5	Программно-аппаратные средства и методы обеспечения информационной безопасности	22	4	-	8	1	9	О
Тема 6	Криптографические методы защиты информации	19	3	-	6	1	9	О
Промежуточная аттестация		-	-	-	-	-	-	Зачет с оценкой
	Всего:	**108**	**16**	**-**	**32**	**6**	**54**	

Примечание: Н – наблюдение, О - опрос.

Содержание дисциплины (модуля)

Тема 1. Введение в информационную безопасность.

Содержание темы:

Информационная безопасность. Основные понятия. Модели информационной безопасности. Виды защищаемой информации.

Тема 2. Правовое обеспечение информационной безопасности.

Содержание темы:

Основные нормативно-правовые акты в области информационной безопасности. Правовые особенности обеспечения безопасности конфиденциальной информации и государственной тайны.

Тема 3. Организационное обеспечение информационной безопасности.

Содержание темы:

Основные стандарты в области обеспечения информационной безопасности. Политика безопасности. Экономическая безопасность предприятия.

Тема 4. Технические средства и методы защиты информации.

Содержание темы:

Инженерная защита объектов. Защита информации от утечки по техническим каналам.

Тема 5. Программно-аппаратные средства и методы обеспечения информационной безопасности.

Содержание темы:

Основные виды сетевых и компьютерных угроз. Средства и методы защиты от сетевых компьютерных угроз.

Тема 6. Криптографические методы защиты информации.

Содержание темы:

Симметричные и ассиметричные системы шифрования. Цифровые подписи (Электронные подписи). Инфраструктура открытых ключей. Криптографические протоколы.

4. Материалы текущего контроля успеваемости обучающихся и фонд оценочных средств промежуточной аттестации по дисциплине (модулю)

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

4.1.1. В ходе реализации дисциплины *Б1.В.ДВ.03.02 Информационная безопасность* **используются следующие методы текущего контроля успеваемости обучающихся:**

При проведении занятий лекционного типа:
устное изложение преподавателем учебного материала.

При проведении практических занятий:
ответы на вопросы преподавателя и выступления с места по тематике семинара

При контроле результатов самостоятельной работы студентов:
изучение вопросов, которые не излагались преподавателем на лекциях и на семинарских (практических) занятиях, работа с литературой.

4.1.2. Зачет проводится в форме подведения итогов по результатам посещения

лекционных и практических занятий, работы на практических занятиях (опрос), ответа на вопросы преподавателя, заданным в устной форме, из списка предложенных.

4. 2. Материалы текущего контроля успеваемости обучающихся.

Вопросы для опроса:

Тема 1. Введение в информационную безопасность.

1. Что такое информационная безопасность?
2. Перечислите основные угрозы информационной безопасности.
3. Какие существуют модели информационной безопасности?
4. Какие методы защиты информации выделяют?
5. Что такое правовые методы защиты информации?
6. Что такое организационные методы защиты информации?
7. Что такое технические методы защиты информации?
8. Что такое программно-аппаратные методы защиты информации?
9. Что такое криптографические методы защиты информации?
10. Что такое физические методы защиты информации?
11. Какие главные государственные органы в области обеспечения информационной безопасности?
12. Перечислите виды защищаемой информации.

Тема 2. Правовое обеспечение информационной безопасности.

1. Какие основные законы в области защиты информации в РФ?
2. Перечислите основные цели и задачи РФ в области обеспечения информационной безопасности
3. Что такое концепция информационной безопасности?
4. Что такое конфиденциальная информация?
5. Что такое персональные данные?
6. В каких случаях возможно использовать персональные данные без согласия обладателя?
7. Охарактеризуйте биометрические данные как персональные данные.
8. Что такое профессиональная тайна?
9. Что такое коммерческая тайна?
10. Что такое режим коммерческой тайны?
11. Что такое государственная тайна?
12. Опишите правовой режим государственной тайны.
13. Какие государственные органы занимаются сертификацией и лицензированием средств защиты информации?

Тема 3. Организационное обеспечение информационной безопасности.

1. Какие основные международные стандарты в области информационной безопасности существуют?
2. Что такое "Единые критерии"
3. Как связаны международные стандарты и стандарты РФ?
4. Какие основные стандарты РФ в области информационной безопасности существуют?
5. Охарактеризуйте стандарт ГОСТ Р ИСО/МЭК 27002-2014.
6. Что такое политика безопасности?
7. Какое количество средств бюджета организации эффективно тратить для обеспечения информационной безопасности?

Тема 4. Технические средства и методы защиты информации.

1. Что такое инженерная защита объектов?

2. Какие виды сигнализаций устанавливаются для обеспечения ин-женерной защиты?
3. Что такое технические каналы утечки информации?
4. Перечислите основные виды технических каналов утечки информации?
5. Перечислите методы защиты информации от утечки по визуальному каналу.
6. Перечислите методы защиты информации от утечки по воздушному каналу.
7. Перечислите методы защиты информации от утечки по вибрационному каналу.
8. Перечислите методы защиты информации от утечки по индукционному каналу.
9. Перечислите средства и методы защиты информации от утечки в телефонных линиях.
10. Перечислите основные мероприятия по обеспечению защиты информации от утечки по техническим каналам.

Тема 5. Программно-аппаратные средства и методы обеспечения информационной безопасности.

1. Какие виды компьютерных угроз существуют?
2. Что такое брандмауэр?
3. Что такое антивирусная программа?
4. Что такое эвристический алгоритм поиска вирусов?
5. Что такое сигнатурный поиск вирусов?
6. Методы противодействия сниффингу?
7. Какие программные реализации программно-аппаратных средств защиты информации вы знаете?
8. Что такое механизм контроля и разграничения доступа?
9. Какую роль несет журналирование действий в программно-аппаратных средствах защиты информации?
10. Что такое средства стеганографической защиты информации?

Тема 6. Криптографические методы защиты информации.

1. Что такое криптография?
2. Какие используются симметричные алгоритмы шифрования?
3. Какие используются ассиметричные алгоритмы шифрования?
4. Что такое криптографическая хеш-функция?
5. Какие используются криптографические хеш-функции?
6. Что такое цифровая подпись?
7. Что такое инфраструктура открытых ключей?
8. Какие российские и международные стандарты на формирование цифровой подписи существуют?
9. Какие основные криптографические протоколы используются в сетях?

4.3. Оценочные средства для промежуточной аттестации.

4.3.1. Формируемые компетенции

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ОПК-1	способностью решать стандартные задачи профессиональной деятельности на основе	ОПК-1.3	Готовность разрабатывать проекты решений по улучшению системы информационной

	информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности		безопасности в соответствии с существующей практикой с учетом результатов аналитической работы. Формирование навыков и развитие навыков прогнозирования и защиты бизнеса от внутренних и внешних вызовов

4.3.2 Типовые оценочные средства

Вопросы к зачету:

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 информа-ции.
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 информа-ции.
18. Программно-аппаратные средства обеспечения информацион-ной 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.

Шкала оценивания.

Оценочным средством промежуточной аттестации является накопительная оценка результатов выполнения текущего контроля по дисциплине.

Максимальный накопленный балл, который может быть достигнут студентом по дисциплине (включая зачет), **составляет 100 баллов**. Конечный балл, набранный

студентом в течение семестра, определяется суммированием полученных баллов по следующим позициям:

	Вид работы	максимально возможный набранный балл
1.	работа на лекциях - посещение	0,5б.*8л.=4б.
2.	работа на практических занятиях - посещение - опрос, выполнение заданий	1б.*16пр.=16б. 3б.*16пр.=48б.
3.	зачет	0-32б.

Для определения конечной оценки по дисциплине набранные студентом баллы переводятся из 100-бальной шкалы в 5-бальную по следующей схеме:

от 0 до 50 включительно	от 51 до 69 включительно	от 70 до 84 включительно	от 85 до 100 включительно
«неудовлетворительно» - 2	«удовлетворительно» - 3	«хорошо» - 4	«отлично» - 5

4.4. Методические материалы

Освоение дисциплины «Информационная безопасность» предусматривает комплекс мероприятий, направленных на формирование у обучающихся системных теоретических знаний и умений решать проблемы принятия оптимальных и рациональных решений в актуальных сферах экономики, социологии, политики и управления, умение заниматься разработкой научно-обоснованных решений в реальных условиях внешней и внутренней среды.

Базовый материал по конкретным вопросам осваиваемой дисциплины дается в рамках занятий лекционного типа.

Целью самостоятельной работы является повторение, закрепление и расширение пройденного материала.

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

В рамках освоения дисциплины предусмотрены следующие формы работы бакалавра: посещение и работа на лекциях и практических занятиях.

Дисциплина разбита на темы, которые представляют собой логически завершенные блоки и являются комплексом знаний и умений, которые подлежат контролю.

В курсе используются классические аудиторные методы проведения занятий. Освоение темы на лекции, при выполнении внеаудиторной (самостоятельной) работы завершается на практическом занятии.

При подготовке к практическим занятиям следует в полной мере использовать литературу, рекомендованную преподавателем. Помимо учебной, научной литературы студентами должны активно использоваться информационные ресурсы, а также словари, справочники. Они дают более углубленное представление о проблемах, получивших систематическое изложение в учебниках. Умение работать с литературой означает научиться осмысленно пользоваться источниками.

Прежде чем приступить к освоению научной литературы, рекомендуется чтение учебников и учебных пособий.

Серьезная и методически грамотно организованная работа студента значительно облегчит подготовку к зачету. Основными функциями зачета являются: обучающая и оценочная. При подготовке к зачету студент повторяет, как правило, ранее изученный материал. В этот период сыграют большую роль правильно подготовленные заранее записи и конспекты. Студенту останется лишь повторить пройденное, учесть, что было

пропущено, восполнить пробелы при подготовке к семинарам, закрепить ранее изученный материал. Зачет позволяет оценить уровень сформированности этапа компетенций.

Методические рекомендации по подготовке к зачету

Подготовка студентов к сдаче зачета включает в себя:

- просмотр программы учебного курса;
- определение необходимых для подготовки источников и их изучение;
- использование методических пособий;
- консультирование у преподавателя.

Подготовка к зачету начинается с первого занятия по дисциплине, на котором студенты получают общую установку преподавателя и перечень основных требований к текущей и итоговой отчетности. При этом важно с самого начала планомерно осваивать материал, руководствуясь, прежде всего перечнем вопросов к зачету, конспектировать важные для решения учебных задач источники. В течение семестра происходит пополнение, систематизация и корректировка студенческих наработок, освоение нового и закрепление уже изученного материала.

Зачет преследует цель оценить работу студента, его теоретические знания и практические навыки, их прочность, развитие творческого мышления, приобретение навыков самостоятельной работы, умения синтезировать полученные знания и применять на практике при решении практических задач.

Самостоятельная работа студентов является важным этапом подготовки к зачету, поскольку студент имеет возможность оценить уровень собственных знаний и своевременно восполнить имеющиеся пробелы.

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. Баранова Е.К. Моделирование системы защиты информации. Практикум: учеб. пособие для студентов вузов / Е. К. Баранова, А. В. Бабаш. - М. : РИОР : ИНФРА-М, 2015. - 120 с. - (Высшее образование : Бакалавриат)
2. Платонов В.В. Программно-аппаратные средства защиты информации: учебник для студентов вузов, обуч. по направл. подгот. "Информ. безопасность" / В. В. Платонов. - 2-е изд., стер. - М. : Академия, 2014. - 336 с.
3. Защита информации: учеб. пособие для студентов вузов (бакалавриат и магистратура) / А. П. Жук, Е. П. Жук, О. М. Лепешкин, А. И. Тимошкин. - М. : РИОР : ИНФРА-М, 2013. - 392 с. - (Высшее образование : Бакалавриат; Магистратура).

6.2. Дополнительная литература.

1. Расторгуев С. П. Основы информационной безопасности: учеб. пособие. М.: Академия, 2009. – 187 с.
2. Технические средства и методы защиты информации: Учебник для вузов / Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.; под ред. А.П. Зайцева и А.А. Шелупанова. – М.: ООО «Издательство Машиностроение», 2009 – 508 с.
3. Практическая криптография: алгоритмы и их программирование / А. В. Аграновский, Р.А. Хади – М.: СОЛОН-Пресс, 2009. - 256 с.

6.3. Учебно-методическое обеспечение самостоятельной работы.

6.4. Нормативные правовые документы.

6.5. Интернет-ресурсы.

1. http://abc.vvsu.ru/ – сайт цифровых учебно-методических материалов Центра

Образования ВГУЭС

2. http://study.vvsu.ru/ – раздаточные материалы для учебного процесса ВГУЭС
3. www.consultant.ru – сайт нормативных документов, предоставляемых компанией "Консультант плюс".

6.6. Иные источники.

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

Учебная аудитория должна быть оснащена наглядными учебными пособиями, экраном, мультимедийным проектором с ноутбуками (ПК) для презентации учебного материала, с выходом в сеть Интернет, программные продукты Microsoft Office (Excel, Word, PowerPoint).