Приложение 3
к основной профессиональной
образовательной программе
по направлению подготовки
38.03.02 Менеджмент
направленность (профиль) программы
Менеджмент на предприятиях ресторанно-
гостиничного бизнеса и туризма

Министерство науки и высшего образования Российской Федерации
федеральное государственное бюджетное образовательное учреждение высшего образования
«Российский экономический университет имени Г.В. Плеханова»

Краснодарский филиал РЭУ им. Г.В. Плеханова

Факультет экономики, менеджмента и торговли

Кафедра бухгалтерского учета и анализа

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.О.ДЭ.02.02 Основы информационной безопасности

Направление подготовки 38.03.02 Менеджмент

Направленность (профиль) программы Менеджмент на предприятиях ресторанно-гостиничного бизнеса и туризма

Уровень высшего образования ***Бакалавриат***

Год начала подготовки 2023

Краснодар – 2022 г.

Составитель(и):
к.п.н., доцент кафедры бухгалтерского учета и анализа Р.Н. Фролов

Рабочая программа одобрена на заседании кафедры бухгалтерского учета и анализа протокол № 6 от 10 января 2022 г.

СОДЕРЖАНИЕ

I. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ

Цель и задачи освоения дисциплины

Цель дисциплины заключается в формировании знаний об объектах и задачах защиты, способах и средствах нарушения информационной безопасности, о принципах и подходах к решению задач защиты информации; а также формирование умений по применению современных технологий, выбора средств и инструментов защиты информации для построения современных защищенных экономических информационных систем.

Задачи дисциплины:

- изучить средства обеспечения информационной безопасности экономической информационной системы современной организации;
- формирование умения обеспечить защиту информации и объектов информатизации; формирование умения составлять заявительную документацию в надзорные государственные органы инфокоммуникационной отрасли;
- изучить средства защиты данных от разрушающих программных воздействий;
- понимать и внедрять организацию комплексной защиты информации на компьютерах организации
- формирование навыков обеспечения защиты объектов интеллектуальной собственности, результатов исследований и разработок как коммерческой тайны предприятия.

2.Содержание дисциплины:

Место дисциплины в структуре образовательной программы

Дисциплина «Основы информационной безопасности», относится к обязательной части учебного плана.

Объем дисциплины и виды учебной работы

Таблица 1

Показатели объема дисциплины	Всего часов по формам обучения	
	очная	***очно-заочная***
Объем дисциплины в зачетных единицах	***3 ЗЕТ***	
Объем дисциплины в акад.часах	***108***	
Промежуточная аттестация: форма	зачет	зачет
Контактная работа обучающихся с преподавателем (Контакт.часы), всего:	**30**	**14**
1. Контактная работа на проведение занятий лекционного и семинарского	28	*12*

типов, всего часов, в том числе:		
• лекции	*12*	*6*
• практические занятия	*16*	*6*
• лабораторные занятия	-	-
в том числе практическая подготовка	-	-
2. Индивидуальные консультации (ИК)***(заполняется при наличии по дисциплине курсовых работ/проектов)*	-	-
3. Контактная работа по промежуточной аттестации (Катт) *(заполняется при наличии по дисциплине курсовых работ/проектов)*	2	2
4. Консультация перед экзаменом (КЭ)	-	-
5. Контактная работа по промежуточной аттестации в период экз. сессии / сессии заочников (Каттэк)	-	-
Самостоятельная работа (СР), всего:	***78***	***94***
в том числе:		
• самостоятельная работа в период экз. сессии (СРэк) (*заполняется при наличии экзамена по дисциплине)*	-	-
• самостоятельная работа в семестре(СРс)	*78*	*94*
в том числе, самостоятельная работа на курсовую работу*(заполняется при наличии по дисциплине курсовых работ/проектов)*	-	-
• изучение ЭОР (*при наличии*)	-	-
• изучение онлайн-курса или его части	-	-
• выполнение индивидуального или группового проекта	-	-
• *и другие виды*	*78*	*94*

Перечень планируемых результатов обучения по дисциплине

Таблица 2

Формируемые компетенции (*код и наименование компетенции*)	**Индикаторы достижения компетенций (*код и наименование индикатора*)**	**Результаты обучения *(знания, умения)***
УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.2. Разрабатывает варианты решения проблемной ситуации на основе критического анализа доступных источников информации	УК-1.2.З-1. **Знает** критерии сопоставления различных вариантов решения поставленной задачи
		УК-1.2.У-1. **Умеет** осуществлять критический анализ собранной информации на соответствие ее условиям и критериям решения поставленной задачи

		УК-1.2.У-2. **Умеет** отличать факты от мнений, интерпретаций и оценок при анализе собранной информации
		УК-1.2.У-3. **Умеет** сопоставлять и оценивать различные варианты решения поставленной задачи, определяя их достоинства и недостатки
ОПК-2. Способен осуществлять сбор, обработку и анализ данных, необходимых для решения поставленных управленческих задач, с использованием современного инструментария и интеллектуальных информационно-аналитических систем	ОПК-2.1. Определяет источники информации и осуществляет их поиск на основе поставленных целей для решения профессиональных задач	ОПК-2.1. З-1. **Знает** методы сбора информации, способы и вид ее представления, применяя современное программное обеспечение
		ОПК-2.1. У-1. **Умеет** использовать современный инструментарий и интеллектуальные информационно-аналитические системы
ОПК-5. Способен использовать при решении профессиональных задач современные информационные технологии и программные средства, включая управление крупными массивами данных и их интеллектуальный анализ	ОПК-5.2. Применяет современные информационные технологии и системы для постановки и решения задач управления, включая управление крупными массивами данных и их интеллектуальный анализ	ОПК-5.2. З-1. **Знает** особенности использования современных информационных технологий и систем для постановки и решения задач управления, включая управление крупными массивами данных и их интеллектуальный анализ
		ОПК-5.2. У-1. **Умеет** решать задачи управления на основе использования современных информационных технологий и систем
ОПК-6. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ОПК-6.1. Использует соответствующие содержанию профессиональных задач современные цифровые информационные технологии, основываясь на принципах их работы	ОПК-6.1. З-1. **Знать**: характеристики соответствующих содержанию профессиональных задач современных цифровых информационных технологий
		ОПК-6.1. У-1. **Уметь**: использовать современные цифровые информационные технологии для решения задач профессиональной деятельности
	ОПК-6.2. Понимает принципы работы современных цифровых информационных технологий, соответствующих содержанию профессиональных задач	ОПК-6.2. З-1**. Знать**: принципы работы соответствующих содержанию профессиональных задач современных цифровых информационных технологий
		ОПК-6.2.У-1. **Умеет** применять принципы работы соответствующих содержанию профессиональных задач современных цифровых информационных технологий

II. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

этапы формирования и критерии оценивания сформированности компетенций
для обучающихся очной формы обучения

Таблица 3.1

№ п/п	Наименование раздела, темы дисциплины	Трудоемкость, академические часы						Индикаторы достижения компетенций	Результаты обучения *(знания, умения)*	Учебные задания для аудиторных занятий	Текущий контроль	Задания для творческого рейтинга (по теме(-ам)/ разделу или по всему куру в целом)
		Лекции	Практические занятия	Лабораторные занятия	Практическая подготовка	Самостоятельная работа/ КЭ, Каттэк, Катт	Всего					
	Семестр 4											
	Раздел 1. Основные определения и понятия информационной безопасности											
1.	**Тема 1. Информация как объект защиты. Правовое обеспечение информационной безопасности** Информационная безопасность. Основные понятия. Модели информационной безопасности. Виды защищаемой информации. Основные нормативно-правовые акты в области информационной безопасности. Правовые особенности обеспечения безопасности конфиденциальной информации и государственной тайны. Ресурсы предприятия, подлежащие защите с точки зрения ИБ. Аспекты ИБ в рамках менеджмента непрерывности бизнеса.	*2*	4			***18***		УК-1.2. ОПК-2.1. ОПК-5.2. ОПК-6.1 ОПК-6.2.	УК-1.2.З-1 УК-1.2.У-1. . УК-1.2.У-2. УК-1.2.У-3. ОПК-2.1. З-1. ОПК-2.1. У-1. ОПК-5.2. З-1. ОПК-5.2. У-1. ОПК-6.1. З-1 ОПК-6.1. У-1. ОПК-6.2. З-1. ОПК-6.2.У-1.	О.		-

2.	**Тема 2. Организационное обеспечение информационной безопасности** Основные стандарты в области обеспечения информационной безопасности. Политика безопасности. Экономическая безопасность предприятия. Инженерная защита объектов. Защита информации от утечки по техническим каналам. Использование баз данных для нахождения и изучения нормативных документов в области информационной безопасности. Идентификация и оценка активов. Модель угроз. Идентификация уязвимостей. Оценка рисков. Обработка рисков. Модель нарушителя политики безопасности. Типичные угрозы информации и уязвимости корпоративных информационных систем.	*4*	4			***18***		УК-1.2. ОПК-2.1. ОПК-5.2. ОПК-6.1 ОПК-6.2.	УК-1.2.З-1 УК-1.2.У-1. . УК-1.2.У-2. УК-1.2.У-3. ОПК-2.1. З-1. ОПК-2.1. У-1. ОПК-5.2. З-1. ОПК-5.2. У-1. ОПК-6.1. З-1 ОПК-6.1. У-1. ОПК-6.2. З-1. ОПК-6.2.У-1.	О.	К.	Д.
Раздел 2. Программно-аппаратные средства и методы обеспечения информационной безопасности												
3.	**Тема 3. Программно-аппаратные средства обеспечения информационной безопасности в информационных сетях** Основные виды сетевых и компьютерных угроз. Средства и методы защиты от сетевых компьютерных угроз. Симметричные и ассиметричные системы шифрования. Цифровые подписи (Электронные подписи). Инфраструктура открытых ключей. Криптографические протоколы.	*2*	***4***			***21***		УК-1.2. ОПК-2.1. ОПК-5.2. ОПК-6.1 ОПК-6.2.	УК-1.2.З-1 УК-1.2.У-1. . УК-1.2.У-2. УК-1.2.У-3. ОПК-2.1. З-1. ОПК-2.1. У-1. ОПК-5.2. З-1. ОПК-5.2. У-1. ОПК-6.1. З-1 ОПК-6.1. У-1. ОПК-6.2. З-1. ОПК-6.2.У-1.	Гр.д.	К.	

4.	**Тема 4. Стандарты и спецификации в области информационной безопасности** Стандартизация в сфере управления информационной безопасностью (на основе международных стандартов ISO/IEC 17799, ISO/IEC27002, ISO/IEC27001,ISO/IEC 15408). Создание зашифрованных файлов и криптоконтейнеров и их расшифрование. Соответствие требованиям законодательства. Соответствие политикам безопасности и стандартам, техническое соответствие. Создание удостоверяющего центра, генерация открытых и секретных ключей, создание сертификатов открытых ключей, создание электронной подписи, проверка электронной подписи.	*4*	***4***			***21***		УК-1.2. ОПК-2.1. ОПК-5.2. ОПК-6.1 ОПК-6.2.	УК-1.2.З-1 УК-1.2.У-1. . УК-1.2.У-2. УК-1.2.У-3. ОПК-2.1. З-1. ОПК-2.1. У-1. ОПК-5.2. З-1. ОПК-5.2. У-1. ОПК-6.1. З-1 ОПК-6.1. У-1. ОПК-6.2. З-1. ОПК-6.2.У-1.	О.	К.р.	
	Контактная работа по промежуточной аттестации (Катт)	-	-	-	-	-/2	2					
	Итого	**12**	**16**	**-**	**-**	**78/2**	**108**					

Этапы формирования и критерии оценивания сформированности компетенций для обучающихся очно-заочной формы обучения

Таблица 3.2

№ п/п	Наименование раздела, темы дисциплины	Трудоемкость, академические часы						Индикаторы достижения компетенций	Результаты обучения *(знания, умения)*	Учебные задания для аудиторных занятий	Текущий контроль	Задания для творческого рейтинга (по теме(-ам)/ разделу или по всему куру в целом)
		Лекции	Практические занятия	Лабораторные занятия	Практическая подготовка	Самостоятельная работа/ КЭ, Каттэк, Катт	Всего					
	Семестр 4											
	Раздел 1. Основные определения и понятия информационной безопасности											

1.	**Тема 1. Информация как объект защиты. Правовое обеспечение информационной безопасности** Информационная безопасность. Основные понятия. Модели информационной безопасности. Виды защищаемой информации. Основные нормативно-правовые акты в области информационной безопасности. Правовые особенности обеспечения безопасности конфиденциальной информации и государственной тайны. Ресурсы предприятия, подлежащие защите с точки зрения ИБ. Аспекты ИБ в рамках менеджмента непрерывности бизнеса.	*2*	2			***23***	27	УК-1.2. ОПК-2.1. ОПК-5.2. ОПК-6.1 ОПК-6.2.	УК-1.2.З-1 УК-1.2.У-1. . УК-1.2.У-2. УК-1.2.У-3. ОПК-2.1. З-1. ОПК-2.1. У-1. ОПК-5.2. З-1. ОПК-5.2. У-1. ОПК-6.1. З-1 ОПК-6.1. У-1. ОПК-6.2. З-1. ОПК-6.2.У-1.	О.		-
2.	**Тема 2. Организационное обеспечение информационной безопасности** Основные стандарты в области обеспечения информационной безопасности. Политика безопасности. Экономическая безопасность предприятия. Инженерная защита объектов. Защита информации от утечки по техническим каналам. Использование баз данных для нахождения и изучения нормативных документов в области информационной безопасности. Идентификация и оценка активов. Модель угроз. Идентификация уязвимостей. Оценка рисков. Обработка рисков. Модель нарушителя политики безопасности. Типичные угрозы информации и уязвимости корпоративных информационных систем.	*2*	2			***23***	27	УК-1.2. ОПК-2.1. ОПК-5.2. ОПК-6.1 ОПК-6.2.	УК-1.2.З-1 УК-1.2.У-1. . УК-1.2.У-2. УК-1.2.У-3. ОПК-2.1. З-1. ОПК-2.1. У-1. ОПК-5.2. З-1. ОПК-5.2. У-1. ОПК-6.1. З-1 ОПК-6.1. У-1. ОПК-6.2. З-1. ОПК-6.2.У-1.	О.	К.	Д.
Раздел 2. Программно-аппаратные средства и методы обеспечения информационной безопасности												

3.	**Тема 3. Программно-аппаратные средства обеспечения информационной безопасности в информационных сетях** Основные виды сетевых и компьютерных угроз. Средства и методы защиты от сетевых компьютерных угроз. Симметричные и ассиметричные системы шифрования. Цифровые подписи (Электронные подписи). Инфраструктура открытых ключей. Криптографические протоколы.	*2*				***24***	26	УК-1.2. ОПК-2.1. ОПК-5.2. ОПК-6.1 ОПК-6.2.	УК-1.2.З-1 УК-1.2.У-1. . УК-1.2.У-2. УК-1.2.У-3. ОПК-2.1. З-1. ОПК-2.1. У-1. ОПК-5.2. З-1. ОПК-5.2. У-1. ОПК-6.1. З-1 ОПК-6.1. У-1. ОПК-6.2. З-1. ОПК-6.2.У-1.	Гр.д.	К.	
4.	**Тема 4. Стандарты и спецификации в области информационной безопасности** Стандартизация в сфере управления информационной безопасностью (на основе международных стандартов ISO/IEC 17799, ISO/IEC27002, ISO/IEC27001,ISO/IEC 15408). Создание зашифрованных файлов и криптоконтейнеров и их расшифрование. Соответствие требованиям законодательства. Соответствие политикам безопасности и стандартам, техническое соответствие. Создание удостоверяющего центра, генерация открытых и секретных ключей, создание сертификатов открытых ключей, создание электронной подписи, проверка электронной подписи.		***2***			***24***	26	УК-1.2. ОПК-2.1. ОПК-5.2. ОПК-6.1 ОПК-6.2.	УК-1.2.З-1 УК-1.2.У-1. . УК-1.2.У-2. УК-1.2.У-3. ОПК-2.1. З-1. ОПК-2.1. У-1. ОПК-5.2. З-1. ОПК-5.2. У-1. ОПК-6.1. З-1 ОПК-6.1. У-1. ОПК-6.2. З-1. ОПК-6.2.У-1.	О.	К.р.	
	Контактная работа по промежуточной аттестации (Катт)	-	-	-	-	-/2	2					
	Итого	**6**	**6**	**-**	**-**	**94/2**	**108**					

Формы учебных заданий на аудиторных занятиях:

Опрос (О)

Групповая дискуссия (Гр.д.)

Формы текущего контроля:

Кейс (К.)

Контрольные работы (К/р)

Формы заданий для творческого рейтинга:

Доклад (Д)

III. УЧЕБНО-МЕТОДИЧЕСКОЕ И МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

Основная литература

1. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 336 с. — (Высшее образование). — DOI: https://doi.org/10.29039/1761-6. - ISBN 978-5-369-01761-6. - Текст: электронный. - URL: https://znanium.com/read?id=364911
2. Клименко, И. С. Информационная безопасность и защита информации: модели и методы управления : монография / И.С. Клименко. — Москва : ИНФРА-М, 2021. — 180 с. — (Научная мысль). — DOI 10.12737/monography_5d412ff13c0b88.75804464. - ISBN 978-5-16-015149-6. - Текст: электронный. - URL: https://znanium.com/read?id=360289
3. Сычев, Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2022. — 201 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/1013711. - ISBN 978-5-16-014976-9. - Текст: электронный. - URL: https://znanium.com/read?id=388766

Дополнительная литература:

1. Международная информационная безопасность: теория и практика : в трех томах. Том 1 : учебник / под общ. ред А. В. Крутских. - 2-е изд., доп. - Москва : Издательство «Аспект Пресс», 2021. - 384 с. - ISBN 978-5-7567-1098-4. - Текст : электронный. - URL: https://znanium.com/read?id=373117
2. Бабаш, А. В. Моделирование системы защиты информации. Практикум : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 3-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 320 с. + Доп. материалы [Электронный ресурс]. — (Высшее образование). — DOI: https://doi.org/10.29039/01848-4. - ISBN 978-5-369-01848-4. - Текст : электронный. - URL: https://znanium.com/read?id=371348
3. Зверева, В. П. Участие в планировании и организации работ по обеспечению защиты объекта : учебник / В.П. Зверева, А.В. Назаров. — Москва : КУРС : ИНФРА-М, 2020. — 320 с. - ISBN 978-5-906818-92-8. - Текст: электронный. - URL: https://znanium.com/read?id=347024
Кибербезопасность в условиях электронного банкинга : практическое пособие / под ред. П. В. Ревенкова. - Москва: Прометей, 2020. - 522 с. - ISBN 978-5-907244-61-0. - Текст: электронный. - URL: https://znanium.com/read?id=374846

Нормативные правовые документы:

1. Федеральный закон от 31 июля 2020 г. № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» [Электрон.ресурс]. – Режим доступа http://www.consultant.ru/document/cons_doc_LAW_358738/
2. "Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы" [Электрон.ресурс]. – Режим доступа http://www.consultant.ru/document/cons_doc_LAW_216363/

ПЕРЕЧЕНЬ ИНФОРМАЦИОННО-СПРАВОЧНЫХ СИСТЕМ

1. Справочно-правовая система «КонсультантПлюс» http://www.consultant.ru/
2. Информационно-правовая система «Гарант» http://garant.ru

ПЕРЕЧЕНЬ ПРОФЕССИОНАЛЬНЫХ БАЗ ДАННЫХ

1. https://rosmintrud.ru/opendata - База открытых данных Минтруда России
2. http://www.fedsfm.ru/opendata - База открытых данных Росфинмониторинга
3. https://www.polpred.com - Электронная база данных "Polpred.com Обзор СМИ"
4. https://fstec.ru/ - Федеральная служба по техническому и экспортному контролю

ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ "ИНТЕРНЕТ", НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1. https://digital.gov.ru/ru/ - информационный ресурс Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации
2. http://citforum.ru/-«Сервер информационных технологий» - on-line библиотека информационных материалов по компьютерным технологиям.
3. http://www.intuit.ru/-Образовательный портал дистанционного обучения.
4. www.coursera.org-Платформа для бесплатных онлайн-лекций (проект по публикации образовательных материалов в интернете, в виде набора бесплатных онлайн-курсов).

ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ, ВКЛЮЧАЯ ПЕРЕЧЕНЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Операционнаясистема Windows 10, Microsoft Office Professional Plus: 2019 год (MS Word, MS Excel, MS Power Point, MS Access)
АнтивирусDr.Web Desktop Security Suite Комплекснаязащита
Браузер Google Chrome
Adobe Premiere
Power DVD
MediaPlayerClassic

МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Дисциплина «Основы информационной безопасности» обеспечена:

для проведения занятий лекционного типа:

- учебной аудиторией, оборудованной учебной мебелью, мультимедийными средствами обучения для демонстрации лекций-презентаций;

для проведения занятий семинарского типа (практические занятия);

- компьютерным классом;
- помещением для самостоятельной работы, оснащенным компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступак электронной информационно-образовательной среде университета.

IV. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

- Методические рекомендации по организации и выполнению внеаудиторной самостоятельной работы.
- Методические указания по выполнению практических работ.

V. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРЫ ОЦЕНИВАНИЯ ЗНАНИЙ ИУМЕНИЙ, ХАРАКТЕРИЗУЮЩИХ ЭТАПЫ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ

Результаты текущего контроля и промежуточной аттестации формируют рейтинговую оценку работы обучающегося. Распределение баллов при формировании рейтинговой оценки работы обучающегося осуществляется в соответствии с «Положением о рейтинговой системе оценки успеваемости и качества знаний студентов в процессе освоения дисциплины «Основы информационной безопасности» в федеральном государственном бюджетном образовательном учреждении высшего образования «Российский экономический университет имени Г.В. Плеханова».

Таблица 4

Виды работ	**Максимальное количество баллов**
Выполнение учебных заданий на аудиторных занятиях	20
Текущий контроль	20
Творческий рейтинг	20
Промежуточная аттестация *(зачет)*	40
ИТОГО	**100**

В соответствии с Положением о рейтинговой системе оценки успеваемости и качества знаний обучающихся «преподаватель кафедры, непосредственно ведущий занятия со студенческой группой, обязан проинформировать группу о распределении рейтинговых баллов по всем видам работ на первом занятии учебного модуля (семестра), количестве модулей по учебной дисциплине, сроках и формах контроля их освоения, форме

промежуточной аттестации, снижении баллов за несвоевременное выполнение выданных заданий. Обучающиеся в течение учебного модуля (семестра) получают информацию о текущем количестве набранных по дисциплине баллов через личный кабинет студента».

VI. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГОКОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Оценочные материалы по дисциплине разработаны в соответствии с Положением об оценочных материалах в федеральном государственном бюджетном образовательном учреждении высшего образования «Российский экономический университет имени Г.В. Плеханова».

Тематика курсовых работ/проектов

«Курсовая работа/проект по дисциплине «Основы информационной безопасности» учебным планом не предусмотрена.

Перечень вопросов 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 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.
28. Что такое информационная безопасность?
29. Перечислите основные угрозы информационной безопасности.
30. Какие существуют модели и методы информационной безопасности?
31. Что такое правовые методы защиты информации?
32. Что такое организационные методы защиты информации?
33. Что такое технические методы защиты информации?
34. Что такое программно-аппаратные методы защиты информации?
35. Что такое криптографические методы защиты информации?
36. Какие главные государственные органы в области обеспечения информационной безопасности?
37. Перечислите виды защищаемой информации.
38. Какие основные законы в области защиты информации в РФ?
39. Перечислите основные цели и задачи РФ в области обеспечения информационной безопасности
40. Что такое концепция информационной безопасности?
41. Что такое конфиденциальная информация?
42. Что такое персональные данные?
43. В каких случаях возможно использовать персональные данные без согласия обладателя?
44. Охарактеризуйте биометрические данные как персональные данные.
45. Что такое профессиональная тайна?
46. Что такое режим коммерческой тайны?
47. Что такое государственная тайна?
48. Опишите правовой режим государственной тайны.
49. Какие государственные органы занимаются сертификацией и лицензированием средств защиты информации?
50. Как связаны международные стандарты и стандарты РФ?
51. Какие основные стандарты РФ в области информационной безопасности существуют?
52. Охарактеризуйте стандарт ГОСТ Р ИСО/МЭК 27002-2014.
53. Что такое политика безопасности?

54. Какое количество средств бюджета организации эффективно тратить для обеспечения информационной безопасности?

55. Что такое инженерная защита объектов?

56. Перечислите основные мероприятия по обеспечению защиты информации от утечки по техническим каналам.

57. Какие виды компьютерных угроз существуют?

58. Что такое брандмауэр?

59. Что такое антивирусная программа?

60. Что такое эвристический алгоритм поиска вирусов?

61. Что такое сигнатурный поиск вирусов?

62. Методы противодействия сниффингу?

63. Какие программные реализации программно-аппаратных средств защиты информации вы знаете?

64. Что такое механизм контроля и разграничения доступа?

65. Какую роль несет журналирование действий в программно-аппаратных средствах защиты информации?

66. Что такое средства стеганографической защиты информации?

67. Что такое криптография?

68. Какие используются симметричные алгоритмы шифрования?

69. Какие используются ассиметричные алгоритмы шифрования?

70. Что такое криптографическая хеш-функция?

71. Какие используются криптографические хеш-функции?

72. Что такое цифровая подпись?

73. Что такое инфраструктура открытых ключей?

74. Какие российские и международные стандарты на формирование цифровой подписи существуют?

75. Какие основные криптографические протоколы используются в сетях?

Типовые практические задания:

1. 1	Обеспечить кибербезопасность удалённой работы сотрудников во время пандемии Определить уязвимости сервисов для видеоконференций, ненадёжность VPN, человеческий фактор и не всегда квалифицированные сотрудники — со всем этим неизбежно сталкивается каждая компания, вынужденная организовать удалённую работу. Проанализировать ситуацию и рассказать, как свести к минимуму риски и устранить последствия низкого уровня киберграмотности
2.	Настройка аудита в Windows для полноценного SOC-мониторинга Описать настройку политики аудита Windows таким образом, чтобы охват мониторинга SOC был полноценным. Рассмотреть оптимальный список политик, а также выделить самое необходимое, отсеяв лишнее.

3.	Как проводить контроль продуктивности, защита от мошенничества и утечек данных при удалённой работе сотрудников? Опасность утечки данных и возможность корпоративного мошенничества — неизбежные спутники вынужденной удалённой работы. Рассмотреть, как можно минимизировать риски и справиться с актуальными задачами контроля сотрудников на «удалёнке».
4.	Описать шесть шагов для обеспечения должного уровня безопасности удалённых сотрудников Оперативно переводя сотрудников на дистанционную работу, нужно учесть сопряжённые с этим сложности и не забыть про попытки киберпреступников использовать уязвимые места. Предложить шесть шагов, которые позволят подойти к этому вопросу подготовленными.
5.	Описать требования ГОСТ 34-й серии в проектах по информационной безопасности Что подразумевает требование «проектировать по ГОСТу», становится ли оно менее обязательным? Что делать, если государственный регулятор не предлагает замену для ГОСТов 34-й серии? Какими стандартами стоит руководствоваться при оформлении проектной документации?
6.	Как выявить атаку злоумышленников в сетевом трафике? Обнаружить действия киберпреступников в корпоративной сети и классифицируем их в соответствии с матрицей MITRE ATT&CK, которая показывает, какие тактики и техники применялись в ходе кибератаки.
7.	Описать Microsoft Security Compliance Toolkit: защита Windows групповыми политиками Рассмотреть подход к информационной безопасности комплексно. Описать инструменты, которые закрыли бы все «дыры» и создали новые. Описать эталонные настройки политик безопасности и инструменты для работы с ними.
8.	Описать процесс настройки удаленки для сотрудников: Быстро, Безопасно, Бесплатно Что необходимо для организации удаленной работы сотрудников. Какие существуют множества решений способных помочь в реализации этой цели. интернет-шлюз ИКС. С его помощью можно организовать безопасный доступ к сети компании, защититься от вирусов и настроить веб-фильтрацию.
9.	Как организовать безопасную удалённую работу во время карантина? Описать процесс перехода на удалённую работу, рассмотреть очевидные риски для информационной безопасности: модификация трафика, перехват паролей и конфиденциальных данных, а также взлом маршрутизаторов и перенаправление пользователей на вредоносные сайты. Проанализировать контрмеры; в качестве одного из вариантов рассмотреть использование виртуальной частной сети (Virtual Private Network, VPN).
10.	Как построить криптотуннель по ГОСТу с минимальными затратами? Обеспечение безопасности при помощи средств криптографической защиты информации (СКЗИ) — не очень сложная задача, если все технологические участки находятся на хост-машине. Однако для того чтобы передавать и шифровать информацию одновременно, необходимо построить грамотный технологический процесс программного обеспечения.
11.	Как обеспечить безопасность IoT-устройств? Интернет вещей (Internet of Things) — уже очевидная реальность для бизнес-процессов компаний и корпоративных инфраструктур. Однако, несмотря на

	огромное количество «умных» устройств, работающих на предприятиях и в промышленных сетях, безопасность IoT зачастую оставляет желать лучшего. Как исправить положение, и рассказать о методах защиты интернета вещей.
12.	Как организовать практику организации безопасного удалённого доступа? Что происходит на рынке безопасного удалённого доступа и как правильно защитить подключение сотрудника к корпоративным ресурсам извне? Как регуляторы влияют на процесс дистанционной работы и нужно ли следить за сотрудником, работающим из дома?
13.	Рассмотреть процесс предотвращения вторжений с помощью межсетевого экрана нового поколения UserGate В составе межсетевого экрана нового поколения UserGate применяется система обнаружения вторжений (СОВ) собственной разработки, созданная внутри компании без использования открытого кода. Сигнатуры системы обнаружения вторжений разрабатываются и верифицируются собственной командой аналитиков центра мониторинга и реагирования UserGate.
14.	Как создать комплексную систему безопасности на основе Fortinet Security Fabric API? Открытый и общедоступный API, предназначенный для интеграции продуктов Fortinet с внешними решениями, позволяет пользователям расширять возможности имеющихся компонентов, а также гибко интегрировать сторонние продукты в единую комплексную среду информационной безопасности предприятия.
15.	Как функционирует межсетевой экран UserGate X1: информационная безопасность в экстремальных физических условиях Корпоративный межсетевой экран UserGate X1 выделяется из линейки продуктов UserGate уникальными физико-техническими характеристиками. Данный программно-аппаратный комплекс (ПАК) эффективен и надёжен в самых суровых условиях эксплуатации: на промышленных объектах, открытом воздухе, транспорте, сохраняя при этом все преимущества платформы обеспечения профессиональной киберзащиты UserGate.
16.	Описать процесс исполнения требований российских регуляторов по контролю сотрудников Финансовые организации обязаны соблюдать требования положений Банка России и приказов ФСТЭК России. Поскольку назвать список этих требований маленьким язык не поворачивается, мы решили рассмотреть предписания руководящих документов и предложить свой вариант — как можно решить те или иные проблемы или хотя бы облегчить свою участь.
17.	Как предотвратить слив базы данных суперпользователями? Привилегированные пользователи баз данных нередко становятся объектами атак хакеров или сами, пользуясь расширенными правами, эксплуатируют информацию не только в служебных целях. Существует несколько эффективных способов закрытия этих уязвимостей, среди которых можно выделить установку DLP-системы, разграничение доступа, а также ограничение прав суперпользователей до необходимых и достаточных, но удобнее всего автоматизировать защиту от возможных утечек информации из баз данных с помощью коробочных решений, например СУБД Jatoba от компании
18.	Как правильно заполнить журнал учёта СКЗИ? Практически любая организация обменивается конфиденциальными данными со своими партнёрами и структурными подразделениями. Для того чтобы

	обеспечить сохранность передаваемой информации, требуются средства криптографической защиты (СКЗИ). Но работа с ними регламентируется инструкцией, которая написана 20 лет назад и уже не отвечает современным реалиям, а некоторые её пункты вызывают сомнения у специалистов.
19.	Как выбрать сервис-провайдера для построения SOC? Спрос на услуги коммерческих центров мониторинга и реагирования на инциденты в области информационной безопасности (Security Operations Center, SOC) растёт прямо пропорционально повышению ИБ-зрелости российского бизнеса. Как следствие, увеличивается число сервисных провайдеров, оказывающих услуги по созданию и сопровождению центров мониторинга и реагирования на инциденты. Выбирать провайдера основываясь на громких обещаниях построить SOC «с нуля» в считаные дни — плохая идея.
20.	Безопасность в одном окне: как оптимизировать реагирование с помощью IRP? Платформа автоматизации реагирования на инциденты в информационной безопасности — Incident Response Platform (IRP) — это относительно новый для нашего рынка инструмент, который позволяет автоматизировать процессы мониторинга и повысить эффективность реагирования на кибератаки. Ниже расскажем о том, как именно IRP помогает специалистам по ИБ и как её подключить.

Типовые тестовые задания:

1. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?

а) Сотрудники
б) Хакеры
в) Атакующие
г) Контрагенты (лица, работающие по договору

2.Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству? Варианты ответа:
а) Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования
б) Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации
в) Улучшить контроль за безопасностью этой информации
г) Снизить уровень классификации этой информации

3.Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?
а) Владельцы данных
б) Пользователи
в) Администраторы
г) Руководство

4.Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?
а) Поддержка высшего руководства
б) Эффективные защитные меры и методы их внедрения
в) Актуальные и адекватные политики и процедуры безопасности
г) Проведение тренингов по безопасности для всех сотрудников.

Примеры вопросов для опроса:

1. Что такое информационная безопасность?
2. Перечислите основные угрозы информационной безопасности.
3. Какие существуют модели и методы информационной безопасности?
4. Что такое правовые методы защиты информации?
5. Что такое организационные методы защиты информации?
6. Что такое технические методы защиты информации?
7. Что такое программно-аппаратные методы защиты информации?
8. Что такое криптографические методы защиты информации?
9. Какие главные государственные органы в области обеспечения информационной безопасности?
10. Перечислите виды защищаемой информации.
11. Какие основные законы в области защиты информации в РФ?
12. Перечислите основные цели и задачи РФ в области обеспечения информационной безопасности
13. Что такое концепция информационной безопасности?
14. Что такое конфиденциальная информация?
15. Что такое персональные данные?
16. В каких случаях возможно использовать персональные данные без согласия обладателя?
17. Охарактеризуйте биометрические данные как персональные данные.
18. Что такое профессиональная тайна?
19. Что такое режим коммерческой тайны?
20. Что такое государственная тайна?
21. Опишите правовой режим государственной тайны.
22. Какие государственные органы занимаются сертификацией и лицензированием средств защиты информации?
23. Как связаны международные стандарты и стандарты РФ?
24. Какие основные стандарты РФ в области информационной безопасности существуют?
25. Охарактеризуйте стандарт ГОСТ Р ИСО/МЭК 27002-2014.
26. Что такое политика безопасности?
27. Какое количество средств бюджета организации эффективно тратить для обеспечения информационной безопасности?
28. Что такое инженерная защита объектов?
29. Перечислите основные мероприятия по обеспечению защиты информации от утечки по техническим каналам.
30. Какие виды компьютерных угроз существуют?
31. Что такое брандмауэр?

32. Что такое антивирусная программа?
33. Что такое эвристический алгоритм поиска вирусов?
34. Что такое сигнатурный поиск вирусов?
35. Методы противодействия сниффингу?
36. Какие программные реализации программно-аппаратных средств защиты информации вы знаете?
37. Что такое механизм контроля и разграничения доступа?
38. Какую роль несет журналирование действий в программно-аппаратных средствах защиты информации?
39. Что такое средства стеганографической защиты информации?
40. Что такое криптография?
41. Какие используются симметричные алгоритмы шифрования?
42. Какие используются ассиметричные алгоритмы шифрования?
43. Что такое криптографическая хеш-функция?
44. Какие используются криптографические хеш-функции?
45. Что такое цифровая подпись?
46. Что такое инфраструктура открытых ключей?
47. Какие российские и международные стандарты на формирование цифровой подписи существуют?
48. Какие основные криптографические протоколы используются в сетях?

Примеры тем групповых дискуссий:

1.Назначение, структура и методика построения разрешительной системы доступа персонала к секретам фирмы.

2 Порядок проведения переговоров и совещаний по конфиденциальным вопросам.

3. Виды и назначение технических средств защиты информации в помещениях, используемых для ведения переговоров и совещаний.

4. Порядок работы с посетителями фирмы, организационные и технические методы защиты секретов фирмы.

5. Порядок защиты информации в рекламной и выставочной деятельности.

6. Организационное обеспечение защиты информации, обрабатываемой средствами вычислительной и организационной техники.

Примеры типовых заданий для контрольной работы:

Тема 1. Угрозы информационной безопасности в сетях организации

Для выбранного объекта защиты информации (например, почтовый сервер, компьютер в бухгалтерии, телефонная база ограниченного пользования на электронных носителях и др) провести анализ защищенности объекта по следующим пунктам вид угроз, характер происхождения угроз, классы каналов несанкционированного получения информации, источники появления угроз,

причины нарушения целостности информации, потенциально возможные злоумышленные действия. Определить класс защиты информации.

Тема 2. Управление инцидентами ИБ и обеспечение непрерывности бизнеса

Рассмотреть нормативную базу управления инцидентами ИБ и обеспечение непрерывности бизнеса. Стандарт ISO 27035. Идентификация, протоколирование, реагирование на инциденты ИБ. Влияние инцидентов ИБ на бизнес-процессы. Средства управления событиями ИБ. SOC-центры ИБ, SIEM-системы управления информацией о безопасности и событиями информационной безопасности, IRP-системы автоматизации реагирования на инциденты информационной безопасности

Управление непрерывностью бизнеса организации.

Тематика докладов:

1 Информационное право и информационная безопасность.

2 Концепция информационной безопасности.

3 Анализ законодательных актов об охране информационных ресурсов открытого доступа.

4 Анализ законодательных актов о защите информационных ресурсов ограниченного доступа.

5 Соотношение понятий: информационные ресурсы, информационные системы и информационная безопасность.

6 Информационная безопасность (по материалам зарубежных источников и литературы).

7 Правовые основы защиты конфиденциальной информации.

8 Экономические основы защиты конфиденциальной информации.

9 Организационные основы защиты конфиденциальной информации.

10 Структура, содержание и методика составления перечня сведений, относящихся к предпринимательской тайне.

11 Составление инструкции по обработке и хранению конфиденциальных документов.

12 Направления и методы защиты документов на бумажных носителях.

13 Направления и методы защиты машиночитаемых документов.

14 Архивное хранение конфиденциальных документов.

15 Направления и методы защиты аудио- и визуальных документов.

16 Порядок подбора персонала для работы с конфиденциальной информацией.

17 Методика тестирования и проведения собеседования с претендентами на должность, связанную с секретами фирмы.

18 Назначение, структура и методика построения разрешительной системы

доступа персонала к секретам фирмы.

19 Порядок проведения переговоров и совещаний по конфиденциальным вопросам.

20 Виды и назначение технических средств защиты информации в помещениях, используемых для ведения переговоров и совещаний.

21 Порядок работы с посетителями фирмы, организационные и технические методы защиты секретов фирмы.

22 Порядок защиты информации в рекламной и выставочной деятельности.

23 Организационное обеспечение защиты информации, обрабатываемой средствами вычислительной и организационной техники.

24 Анализ источников, каналов распространения и каналов утечки информации (на примере конкретной фирмы).

25 Анализ конкретной автоматизированной системы, предназначенной для обработки и хранения информации о конфиденциальных документах фирмы.

26 Основы технологии обработки и хранения конфиденциальных документов (по зарубежной литературе).

27 Назначение, виды, структура и технология функционирования системы защиты информации.

28 Поведение персонала и охрана фирмы в экстремальных ситуациях различных типов.

29 Аналитическая работа по выявлению каналов утечки информации фирмы.

30 Направления и методы защиты профессиональной тайны.

31 Направления и методы защиты служебной тайны.

32 Направления и методы защиты персональных данных о гражданах.

33 Построение и функционирование защищенного документооборота

Типовая структура зачетного задания

Наименование оценочного материала	***Максимальное количество баллов***
Вопрос 1. Определить место информационной безопасности в обеспечении системы общественной безопасности	*15*
Вопрос 2 Охарактеризовать уровни реализации информационной безопасности	*15*
Практическое задание. Описать характер действия организационных каналов несанкционированного доступа к информации. Раскрыть последовательность условия и формы допуска должностных лиц к государственной тайне	*10*

Показатели и критерии оценивания планируемых результатов освоения компетенций и результатов обучения, шкала оценивания

Таблица 5

Шкала оценивания		Формируемые компетенции	Индикатор достижения компетенции	Критерии оценивания	Уровень освоения компетенций
85 – 100 баллов	**«зачтено»**	**УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач**	УК-1.2. Разрабатывает варианты решения проблемной ситуации на основе критического анализа доступных источников информации	**Знает верно и в полном объеме:** критерии сопоставления различных вариантов решения поставленной задачи	**Продвинутый**
				Умеет верно и в полном обеме: осуществлять критический анализ собранной информации на соответствие ее условиям и критериям решения поставленной задачи; отличать факты от мнений, интерпретаций и оценок при анализе собранной информации; сопоставлять и оценивать различные варианты решения поставленной задачи, определяя их достоинства и недостатки	
		ОПК-2. Способен осуществлять сбор, обработку и анализ данных, необходимых для решения поставленных управленческих задач, с использованием современного инструментария и интеллектуальных информационно-аналитических систем	ОПК-2.1. Определяет источники информации и осуществляет их поиск на основе поставленных целей для решения профессиональных задач	**Знает верно и в полном объеме:** методы сбора информации, способы и вид ее представления, применяя современное программное обеспечение	
				Умеет верно и в полном объеме: использовать современный инструментарий и интеллектуальные информационно-аналитические системы	
		ОПК-5. Способен использовать при решении профессиональных задач современные информационные технологии и программные средства, включая управление крупными массивами данных и их интеллектуальный	ОПК-5.2. Применяет современные информационные технологии и системы для постановки и решения задач управления, включая управление крупными массивами данных и их	**Знает верно и в полном объеме:** особенности использования современных информационных технологий и систем для постановки и решения задач управления, включая управление крупными массивами данных и их интеллектуальный анализ	
				Умеет верно и в полном объеме: решать задачи управления на основе использования современных информационных технологий и систем	

		анализ	интеллектуальный анализ		
		ОПК-6. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ОПК-6.1. Использует соответствующие содержанию профессиональных задач современные цифровые информационные технологии, основываясь на принципах их работы	**Знает верно и в полном объеме:**: характеристики соответствующих содержанию профессиональных задач современных цифровых информационных технологий	
				Умеет верно и в полном объеме: использовать современные цифровые информационные технологии для решения задач профессиональной деятельности	
			ОПК-6.2. Понимает принципы работы современных цифровых информационных технологий, соответствующих содержанию профессиональных задач	**Знает верно и в полном объеме**: принципы работы соответствующих содержанию профессиональных задач современных цифровых информационных технологий	
				Умеет верно и в полном объеме: применять принципы работы соответствующих содержанию профессиональных задач современных цифровых информационных технологий	
70 – 84 баллов	**«зачтено»**	**УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач**	УК-1.2. Разрабатывает варианты решения проблемной ситуации на основе критического анализа доступных источников информации	**Знает с незначительными замечаниями:** критерии сопоставления различных вариантов решения поставленной задачи	**Повышенный**
				Умеет с незначительными замечаниями: осуществлять критический анализ собранной информации на соответствие ее условиям и критериям решения поставленной задачи; отличать факты от мнений, интерпретаций и оценок при анализе собранной информации; сопоставлять и оценивать различные варианты решения поставленной задачи, определяя их достоинства и недостатки	

		ОПК-2. Способен осуществлять сбор, обработку и анализ данных, необходимых для решения поставленных управленческих задач, с использованием современного инструментария и интеллектуальных информационно-аналитических систем	ОПК-2.1. Определяет источники информации и осуществляет их поиск на основе поставленных целей для решения профессиональных задач	**Знает с незначительными замечаниями:** методы сбора информации, способы и вид ее представления, применяя современное программное обеспечение	
				Умеет с незначительными замечаниями : использовать современный инструментарий и интеллектуальные информационно-аналитические системы	
		ОПК-5. Способен использовать при решении профессиональных задач современные информационные технологии и программные средства, включая управление крупными массивами данных и их интеллектуальный анализ	ОПК-5.2. Применяет современные информационные технологии и системы для постановки и решения задач управления, включая управление крупными массивами данных и их интеллектуальный анализ	**Знает с незначительными замечаниями:** особенности использования современных информационных технологий и систем для постановки и решения задач управления, включая управление крупными массивами данных и их интеллектуальный анализ	
				Умеет с незначительными замечаниями: решать задачи управления на основе использования современных информационных технологий и систем	
		ОПК-6. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ОПК-6.1. Использует соответствующие содержанию профессиональных задач современные цифровые информационные технологии, основываясь на принципах их работы	**Знает с незначительными замечаниями:**: характеристики соответствующих содержанию профессиональных задач современных цифровых информационных технологий	
				Умеет с незначительными замечаниями: использовать современные цифровые информационные технологии для решения задач профессиональной деятельности	
			ОПК-6.2. Понимает принципы работы современных цифровых информационных технологий, соответствующих содержанию профессиональных задач	**Знает с незначительными замечаниями**: принципы работы соответствующих содержанию профессиональных задач современных цифровых информационных технологий	
				Умеет с незначительными замечаниями: применять принципы работы соответствующих содержанию профессиональных задач современных цифровых информационных технологий	

50 – 69 баллов	**«зачтено»**	**УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач**	УК-1.2. Разрабатывает варианты решения проблемной ситуации на основе критического анализа доступных источников информации	**Знает на базовом уровне, с ошибками:** критерии сопоставления различных вариантов решения поставленной задачи	**Базовый**
				Умеет на базовом уровне, с ошибками: осуществлять критический анализ собранной информации на соответствие ее условиям и критериям решения поставленной задачи; отличать факты от мнений, интерпретаций и оценок при анализе собранной информации; сопоставлять и оценивать различные варианты решения поставленной задачи, определяя их достоинства и недостатки	
		ОПК-2. Способен осуществлять сбор, обработку и анализ данных, необходимых для решения поставленных управленческих задач, с использованием современного инструментария и интеллектуальных информационно-аналитических систем	ОПК-2.1. Определяет источники информации и осуществляет их поиск на основе поставленных целей для решения профессиональных задач	**Знает на базовом уровне, с ошибками:** методы сбора информации, способы и вид ее представления, применяя современное программное обеспечение	
				Умеет на базовом уровне, с ошибками: использовать современный инструментарий и интеллектуальные информационно-аналитические системы	
		ОПК-5. Способен использовать при решении профессиональных задач современные информационные технологии и программные средства, включая управление крупными массивами данных и их интеллектуальный анализ	ОПК-5.2. Применяет современные информационные технологии и системы для постановки и решения задач управления, включая управление крупными массивами данных и их интеллектуальный анализ	**Знает на базовом уровне, с ошибками:** особенности использования современных информационных технологий и систем для постановки и решения задач управления, включая управление крупными массивами данных и их интеллектуальный анализ	
				Умеет на базовом уровне, с ошибками: решать задачи управления на основе использования современных информационных технологий и систем	
		ОПК-6. Способен понимать принципы работы современных информационных технологий и	ОПК-6.1. Использует соответствующие содержанию профессиональных задач современные	**Знает на базовом уровне, с ошибками:**: характеристики соответствующих содержанию профессиональных задач современных цифровых информационных технологий	

		использовать их для решения задач профессиональной деятельности	цифровые информационные технологии, основываясь на принципах их работы	**Умеет на базовом уровне, с ошибками**: использовать современные цифровые информационные технологии для решения задач профессиональной деятельности	
			ОПК-6.2. Понимает принципы работы современных цифровых информационных технологий, соответствующих содержанию профессиональных задач	**Знает на базовом уровне, с ошибками**: принципы работы соответствующих содержанию профессиональных задач современных цифровых информационных технологий	
				Умеет на базовом уровне, с ошибками: применять принципы работы соответствующих содержанию профессиональных задач современных цифровых информационных технологий	
менее 50 баллов	**«не зачтено»**	**УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач**	УК-1.2. Разрабатывает варианты решения проблемной ситуации на основе критического анализа доступных источников информации	**Не знает на базовом уровне:** критерии сопоставления различных вариантов решения поставленной задачи	**Компетенции не сформированы**
				Не умеет на базовом уровне осуществлять критический анализ собранной информации на соответствие ее условиям и критериям решения поставленной задачи; отличать факты от мнений, интерпретаций и оценок при анализе собранной информации; сопоставлять и оценивать различные варианты решения поставленной задачи, определяя их достоинства и недостатки	
		ОПК-2. Способен осуществлять сбор, обработку и анализ данных, необходимых для решения поставленных управленческих задач, с использованием современного инструментария и интеллектуальных информационно-аналитических систем	ОПК-2.1. Определяет источники информации и осуществляет их поиск на основе поставленных целей для решения профессиональных задач	**Не знает на базовом уровне:** методы сбора информации, способы и вид ее представления, применяя современное программное обеспечение	
				Не умеет на базовом уровне: использовать современный инструментарий и интеллектуальные информационно-аналитические системы	
		ОПК-5. Способен использовать при решении профессиональных задач современные информационные технологии и программные	ОПК-5.2. Применяет современные информационные технологии и системы для постановки и решения задач	**Не знает на базовом уровне:** особенности использования современных информационных технологий и систем для постановки и решения задач управления, включая управление крупными массивами данных и их интеллектуальный анализ	

		средства, включая управление крупными массивами данных и их интеллектуальный анализ	управления, включая управление крупными массивами данных и их интеллектуальный анализ	**Не умеет на базовом уровне:** решать задачи управления на основе использования современных информационных технологий и систем	
		ОПК-6. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ОПК-6.1. Использует соответствующие содержанию профессиональных задач современные цифровые информационные технологии, основываясь на принципах их работы	**Не знает на базовом уровне:**: характеристики соответствующих содержанию профессиональных задач современных цифровых информационных технологий	
				Не умеет на базовом уровне: использовать современные цифровые информационные технологии для решения задач профессиональной деятельности	
			ОПК-6.2. Понимает принципы работы современных цифровых информационных технологий, соответствующих содержанию профессиональных задач	**Не знает на базовом уровне**: принципы работы соответствующих содержанию профессиональных задач современных цифровых информационных технологий	
				Не умеет на базовом уровне: применять принципы работы соответствующих содержанию профессиональных задач современных цифровых информационных технологий	

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Российский экономический университет имени Г.В. Плеханова»
Краснодарский филиал РЭУ им. Г. В. Плеханова

Факультет экономики, менеджмента и торговли

Кафедра бухгалтерского учета и анализа

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

Б1.О.ДЭ.02.02 Основы информационной безопасности

Направление подготовки 38.03.02 Менеджмент

направление (профиль) программы Менеджмент на предприятиях ресторанно-гостиничного бизнеса и туризма

Уровень высшего образования *Бакалавриат*

Краснодар – 2022 г.

1.Цель и задачи дисциплины:

Цель дисциплины заключается в формировании знаний об объектах и задачах защиты, способах и средствах нарушения информационной безопасности, о принципах и подходах к решению задач защиты информации; а также формирование умений по применению современных технологий, выбора средств и инструментов защиты информации для построения современных защищенных экономических информационных систем.

Задачи дисциплины:

- изучить средства обеспечения информационной безопасности экономической информационной системы современной организации;
- формирование умения обеспечить защиту информации и объектов информатизации; формирование умения составлять заявительную документацию в надзорные государственные органы инфокоммуникационной отрасли;
- изучить средства защиты данных от разрушающих программных воздействий;
- понимать и внедрять организацию комплексной защиты информации на компьютерах организации
- формирование навыков обеспечения защиты объектов интеллектуальной собственности, результатов исследований и разработок как коммерческой тайны предприятия.

2.Содержание дисциплины:

№ п/п	Наименование разделов / тем дисциплины
	Раздел 1. Основные определения и понятия информационной безопасности
1.	Тема 1. Информация как объект защиты. Правовое обеспечение информационной безопасности
2.	Тема 2. Организационное обеспечение информационной безопасности
	Раздел 2. Программно-аппаратные средства и методы обеспечения информационной безопасности
4	Тема 4. Программно-аппаратные средства обеспечения информационной безопасности в информационных сетях.
5.	Тема 5. Стандарты и спецификации в области информационной безопасности
Трудоемкость дисциплины составляет 3 з.е. / 108 часа.	

Форма контроля – зачет.

Составитель:

Доцент кафедры бухгалтерского учета и анализа Краснодарского филиала РЭУ им. Г.В. Плеханова, к.п.н. Фролов Р.Н.