

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Петровская Анна Викторовна

Должность: Директор

Дата подписания: 22.07.2026 14:47:23

Уникальный программный ключ:

798bda6555fbdebe827768f6f1710bd17a9070c31fdc1b6a6ac5a1f10c8c5199

*Приложение 3 к основной профессиональной образовательной программе
по направлению подготовки 38.03.01 Экономика
направленность (профиль) программы
«Экономика и управление на предприятии (организации)»*

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 экономики и цифровых технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.О.ДЭ.02.02 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Направления подготовки - 38.03.01 Экономика

**Направленность (профиль) программы «Экономика и управление
на предприятии (организации)»**

Уровень высшего образования - Бакалавриат

Год начала подготовки 2026

Краснодар – 2025 г.

Составитель:

к.т.н., доцент кафедры экономики и цифровых технологий Р.Н. Фролов

Рабочая программа одобрена на заседании кафедры экономики и цифровых технологий, протокол № 8 от 20.03.2025 г.

СОДЕРЖАНИЕ

I. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ	4
Цель и задачи освоения дисциплины	4
Место дисциплины в структуре образовательной программы	4
Объем дисциплины и виды учебной работы	4
Перечень планируемых результатов обучения по дисциплине	5
II. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ	7
III. УЧЕБНО-МЕТОДИЧЕСКОЕ И МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ	12
РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА	12
ПЕРЕЧЕНЬ ИНФОРМАЦИОННО-СПРАВОЧНЫХ СИСТЕМ	12
ПЕРЕЧЕНЬ ПРОФЕССИОНАЛЬНЫХ БАЗ ДАННЫХ	13
ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ "ИНТЕРНЕТ", НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ	13
ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ, ВКЛЮЧАЯ ПЕРЕЧЕНЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ	13
МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ	13
IV. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ	14
V. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРЫ ОЦЕНИВАНИЯ ЗНАНИЙ И УМЕНИЙ, ХАРАКТЕРИЗУЮЩИХ ЭТАПЫ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ	14
VI. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ	15
АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ	27

І. 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

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 типов, всего часов, в том числе:	28	12
• лекции	12	6

• практические занятия	16	6
• лабораторные занятия	-	-
в том числе практическая подготовка	-	-
2. Индивидуальные консультации (ИК)	-	-
3. Контактная работа по промежуточной аттестации (Катт)	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)		
• самостоятельная работа в семестре(СРс)	78	94

Таблица 1

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-1.1. Осуществляет поиск необходимой информации, опираясь на результаты анализа поставленной задачи	УК-1.1. 3-1. Знает основные методы критического анализа и основы системного подхода как общенаучного метода.
		УК-1.1. У-1. Умеет анализировать задачу, используя основы критического анализа и системного подхода.
		УК-1.1. У-2. Умеет осуществлять поиск необходимой для решения поставленной задачи информации, критически оценивая надежность различных источников информации.
ОПК-2. Способен осуществлять сбор, обработку и статистический анализ данных, необходимых для решения поставленных экономических задач	ОПК-2.1. Использует основные методы, средства получения, представления, хранения и обработки статистических данных.	ОПК-2.1. 3-1. Знает методы поиска и систематизации информации об экономических процессах и явлениях
		ОПК-2.1. У-1. Умеет работать с национальными и международными базами данных с целью поиска информации, необходимой для решения поставленных экономических задач.

		ОПК-2.1.У-2. Умеет рассчитывать экономические и социально-экономические показатели, характеризующие деятельность хозяйствующих субъектов на основе типовых методик и действующей нормативно-правовой базы
		ОПК-2.1.У-3. Умеет представить наглядную визуализацию данных.
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. 3-1. Знает: характеристики соответствующих содержанию профессиональных задач современных цифровых информационных технологий
		ОПК-6.1. У-1. Умеет: 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. 3-1. Знает: 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 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	2	4			18	24	УК-1.1. ОПК-2.1.. ОПК-6.1 ОПК-6.2.	УК-1.1. 3-1 УК-1.1. У-1. УК-1.1. У-2. ОПК-2.1. 3-1. ОПК-2.1. У-1 ОПК-2.1. У-2. ОПК-2.1. У-3. ОПК-6.1. 3-1. ОПК-6.1. У-1. ОПК-6.2. 3-1 ОПК-6.2. У-1.	Гр.д.	-	Д

	менеджмента непрерывности бизнеса.											
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	26	УК-1.1. ОПК-2.1.. ОПК-6.1 ОПК-6.2.	УК-1.1. 3-1 УК-1.1. У-1. УК-1.1. У-2. ОПК-2.1. 3-1. ОПК-2.1. У-1 ОПК-2.1. У-2. ОПК-2.1. У-3. ОПК-6.1. 3-1. ОПК-6.1. У-1. ОПК-6.2. 3-1 ОПК-6.2. У-1.	Гр.д.	Р.а,з.	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	27	УК-1.1. ОПК-2.1.. ОПК-6.1 ОПК-6.2.	УК-1.1. 3-1 УК-1.1. У-1. УК-1.1. У-2. ОПК-2.1. 3-1. ОПК-2.1. У-1 ОПК-2.1. У-2. ОПК-2.1. У-3. ОПК-6.1. 3-1. ОПК-6.1. У-1. ОПК-6.2. 3-1 ОПК-6.2. У-1.	Гр.д.	Р.а,з.	Д
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.	4	4			21	29	УК-1.1. ОПК-2.1.. ОПК-6.1 ОПК-6.2.	УК-1.1. 3-1 УК-1.1. У-1. УК-1.1. У-2. ОПК-2.1. 3-1. ОПК-2.1. У-1 ОПК-2.1. У-2. ОПК-2.1. У-3. ОПК-6.1. 3-1. ОПК-6.1. У-1. ОПК-6.2. 3-1 ОПК-6.2. У-1.	Гр.д.	К.р., Т	Д

	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.								ОПК-6.2. 3-1 ОПК-6.2. У-1.			
	<i>Контактная работа по промежуточной аттестации (Катт)</i>	-	-	-	-	-/2	2					
	<i>Самостоятельная работа в период экз. сессии (СРэк)</i>	-	-	-	-	-	-					
	Итого	12	16	-	-	78/2	108	х	х	х	х	х

**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 курсу 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	1	1			22	24	УК-1.1. ОПК-2.1.. ОПК-6.1 ОПК-6.2.	УК-1.1. 3-1 УК-1.1. У-1. УК-1.1. У-2. ОПК-2.1. 3-1. ОПК-2.1. У-1 ОПК-2.1. У-2.	Гр.д.	-	-

	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.								ОПК-2.1. У-3. ОПК-6.1. 3-1. ОПК-6.1. У-1. ОПК-6.2. 3-1 ОПК-6.2. У-1.			
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.	1	1			24	26	УК-1.1. ОПК-2.1.. ОПК-6.1 ОПК-6.2.	УК-1.1. 3-1 УК-1.1. 3-1 УК-1.1. У-1. УК-1.1. У-2. ОПК-2.1. 3-1. ОПК-2.1. У-1 ОПК-2.1. У-2. ОПК-2.1. У-3. ОПК-6.1. 3-1. ОПК-6.1. У-1. ОПК-6.2. 3-1 ОПК-6.2. У-1.	Гр.д.	Р.а,з.	-
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	2			23	27	УК-1.1. ОПК-2.1.. ОПК-6.1 ОПК-6.2.	УК-1.1. 3-1 УК-1.1. У-1. УК-1.1. У-2. ОПК-2.1. 3-1. ОПК-2.1. У-1 ОПК-2.1. У-2. ОПК-2.1. У-3. ОПК-6.1. 3-1. ОПК-6.1. У-1. ОПК-6.2. 3-1 ОПК-6.2. У-1.	Гр.д.	Р.а,з.	-

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	2			25	29	УК-1.1. ОПК-2.1.. ОПК-6.1 ОПК-6.2.	УК-1.1. 3-1 УК-1.1. У-1. УК-1.1. У-2. ОПК-2.1. 3-1. ОПК-2.1. У-1 ОПК-2.1. У-2. ОПК-2.1. У-3. ОПК-6.1. 3-1. ОПК-6.1. У-1. ОПК-6.2. 3-1 ОПК-6.2. У-1..	Гр.д.	К.р., Т	-
	<i>Контактная работа по промежуточной аттестации (Катт)</i>	-	-	-	-	-/2	2					
	<i>Самостоятельная работа в период экз. сессии (СРэк)</i>	-	-	-	-	-	-					
	Итого	6	6	-	-	94/2	108	х	х	х	х	х

Формы учебных заданий на аудиторных занятиях:

Групповая дискуссия (Гр.д.)

Формы текущего контроля:

Контрольная работа (К.р.)

Тест (Т)

Расчетно-аналитическое задание(Р.а,з.)

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, 2024. — 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, 2023. — 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, 2025. — 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, 2022. — 320 с. - ISBN 978-5-906818-92-8. - Текст: электронный. - URL: <https://znanium.com/read?id=347024>

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. <http://www.consultant.ru> -Справочно-правовая система Консультант Плюс;
2. <http://www.garant.ru>- Справочно-правовая система Гарант.

ПЕРЕЧЕНЬ ПРОФЕССИОНАЛЬНЫХ БАЗ ДАННЫХ

1. <http://www.iep.ru/ru/publikacii/categories.html> **Федеральный** образовательный портал. Экономика. Социология. Менеджмент
2. <https://rosmintrud.ru/opendata> - База открытых данных Минтруда России
3. <http://www.fedsfm.ru/opendata> - База открытых данных Росфинмониторинга
4. <https://www.polpred.com> - Электронная база данных "Polpred.com Обзор СМИ"
5. <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

Операционная система Windows 10, Microsoft Office Professional Plus: 2019 год (MS Word, MS Excel, MS Power Point, MS Access)

Антивирус Dr.Web Desktop Security Suite Комплексная защита

Браузер Google Chrome

Adobe Premiere

Power DVD

Media Player Classic

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 доступа к 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 И УМЕНИЙ, 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 обучающегося».

VI. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ 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:

Перечень вопросов к зачету:

1. Необходимость обеспечения безопасности в информационных системах.
2. Меры предупреждения преступлений в сфере компьютерной информации.
3. Прогресс информационных технологий и информационная безопасность.
4. История вредоносных программ.
5. Нормативно-правовые аспекты информационной безопасности.
6. Защита учетной информации коммерческих фирм.
7. Классификация угроз безопасности информационных объектов.
8. Свойства экономической информации, нарушаемые при несанкционированном доступе.
9. Основные виды каналов утечки информации.
10. Исторические аспекты компьютерных преступлений.
11. Умышленные и неумышленные угрозы информационной безопасности.
12. Экономическая информация как объект безопасности.
13. Внешние угрозы информационной безопасности.
14. Перечень сведений, которые не могут составлять коммерческую тайну.
15. Мотивы и цели компьютерных преступлений.
16. Виды тайн и как их сохранить.
17. Статьи уголовного кодекса о компьютерных преступлениях.
18. Причины разглашения конфиденциальной информации.
19. Криминологическая характеристика преступлений в сфере компьютерной информации и их предупреждение.
20. Разглашение и утечка информации.
21. Объекты информационной безопасности на предприятии.
22. Стратегия злоумышленника при несанкционированном доступе.
23. Организационные методы обеспечения информационной безопасности.
24. Организация конфиденциального делопроизводства.

25. Физическая защита информационных систем.
26. Структура службы безопасности компании.
27. Программно - технические методы обеспечения информационной безопасности.
28. Теоретические аспекты информационной безопасности экономических систем.
29. Идентификация и аутентификация.
30. Основные понятия информационной безопасности экономических систем.
31. Доктрина информационной безопасности Российской Федерации.
32. Экономическая информация как товар и объект безопасности.
33. Государственное регулирование информационной безопасности в России.
34. Понятия информационных угроз и их виды.
35. Несанкционированный доступ и защита от него.
36. Вредоносные программы.
37. Проблема информационной безопасности в историческом аспекте.
38. Компьютерные преступления и наказания.
39. Предупреждение компьютерных преступлений.
40. Принципы построения системы информационной безопасности.
41. Типы компьютерных вирусов и защита от них.
42. Подходы, принципы, методы и средства обеспечения безопасности.
43. Человеческие факторы, обуславливающие информационные угрозы.
44. Организационно-техническое обеспечение компьютерной безопасности.
45. Способы воздействия угроз на информационный объект.
46. Электронная цифровая подпись и особенности ее применения.
47. Признаки воздействия вирусов на компьютерную систему.
48. Защита информации в Интернете.
49. Фрагментарный и системный подходы к защите информации.
50. Организация системы защиты информации экономических систем.
51. Уголовно-правовая характеристика компьютерных преступлений.
52. Этапы построения системы защиты информации.
53. Субъективная сторона компьютерных преступлений.
54. Политика безопасности.
55. Объективная сторона компьютерных преступлений.
56. Оценка эффективности инвестиций в информационную безопасность.
57. Способы совершения компьютерных преступлений («за хвост», «маскарад» и др.).
58. Обеспечение информационной безопасности автоматизированных банковских систем (АБС).
59. Причины и условия, способствующие совершению компьютерных преступлений.
60. Информационная безопасность электронной коммерции (ЭК).
61. Обеспечение компьютерной безопасности учетной информации.

Практические задания к зачету

- | |
|--|
| <p>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</p> |
| <p>2. Настройка аудита в Windows для полноценного SOC-мониторинга</p> |

Описать настройку политики аудита Windows таким образом, чтобы охват мониторинга SOC был полноценным. Рассмотреть оптимальный список политик, а также выделить самое необходимое, отсеив 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.

Типовые тестовые задания:

Тема 4. Стандарты и спецификации в области информационной безопасности

1. Контрольные функции в области государственной безопасности по вопросам предотвращения несанкционированного доступа к информации реализуются:

- А. ФСТЭК РФ
- Б. ФСБ РФ
- В. Управлением «К» МВД РФ
- Г. Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций

2. Защита информации от несанкционированного доступа - это:

А. защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленными нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации

Б. деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию

В. защита информации, заключающаяся в обеспечении некриптографическими методами

безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств

Г. защита информации с помощью ее криптографического преобразования

3. Несанкционированный доступ к информации – это...

А. доступ к информации ресурсам информационной системы, осуществляемый с нарушением установленных прав и/или правил доступа к информации ресурсам информационной системы с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному назначению и техническим характеристикам

Б. неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации

В. неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных

Г. изменение, уничтожение или копирование информации (ресурсов информационной системы), осуществляемое с нарушением установленных прав и (или) правил

4. Информационное право составляет:

- А. нормативную базу информационного общества
- Б. государственную политику
- В. нормативную базу аграрного общества
- Г. нормативную базу до индустриального общества

5. Кто такие "киберсквоттеры"?

- А. сетевые деятели, пытающиеся вести паразитическое существование - вирусы
- Б. роботы в сети
- В. сетевые группы по интересам

Примеры тем групповых дискуссий:

Тема 1. Информация как объект защиты. Правовое обеспечение информационной

безопасности

1. Информационная безопасность. Основные понятия.
2. Модели информационной безопасности.
3. Виды защищаемой информации.
4. Основные нормативно-правовые акты в области информационной безопасности.
5. Правовые особенности обеспечения безопасности конфиденциальной информации и государственной тайны.
6. Ресурсы предприятия, подлежащие защите с точки зрения ИБ.
7. Аспекты ИБ в рамках менеджмента непрерывности бизнеса
8. Кибербезопасность и киберпространство..
9. Задачи кибербезопасности в автоматизированных системах.
10. Понятие информации и информатизации, свойства информации как объекта защиты от киберугроз.

Примеры типовых расчетно-аналитических заданий

Тема 2. Организационное обеспечение информационной безопасности

Задание 1.

Поиск источников информации в сети Интернет: открытые и закрытые источники данных. Портал открытых данных РФ. Сохранение данных в программе Excel. Преобразование и первичная обработка данных.

Задание 2.

Безопасность информационных систем

Вопросы:

1. Что вы представляете под безопасностью информационных систем.
2. Что относится к основным характеристикам защищаемой информации?
3. Что вы отнесете к информации ограниченного доступа?
4. По каким направлениям будет осуществляться дальнейшее развитие системы информационной безопасности в РФ?

Задание:

Определите в каких формах представлена информация на вашем домашнем компьютере.

Опишите как обеспечивается информационная безопасность на вашем домашнем компьютере и отвечает ли современным требованиям развития систем безопасности.

Примеры типовых заданий для контрольной работы:

Вариант 1.

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.

Вариант 2.

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.

Тематика докладов по темам 1-4

- 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 Анализ источников, каналов распространения и каналов утечки информации (на примере конкретной фирмы).
- 19 Анализ конкретной автоматизированной системы, предназначенной для обработки и хранения информации о конфиденциальных документах фирмы.
- 20 Основы технологии обработки и хранения конфиденциальных документов (по зарубежной литературе).
- 21 Назначение, виды, структура и технология функционирования системы защиты информации.
- 22 Поведение персонала и охрана фирмы в экстремальных ситуациях различных типов.
- 23 Аналитическая работа по выявлению каналов утечки информации фирмы.
- 24 Направления и методы защиты профессиональной тайны.
- 25 Направления и методы защиты служебной тайны.
- 26 Направления и методы защиты персональных данных о гражданах.
- 27 Построение и функционирование защищенного документооборота

Типовая структура зачетного задания

Наименование оценочного материала	Максимальное количество баллов
<i>Вопрос 1.</i>	<i>15</i>
<i>Вопрос 2.</i>	<i>15</i>
<i>Практическое задание.</i>	<i>10</i>

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-1.1. Осуществляет поиск необходимой информации, опираясь на результаты анализа поставленной задачи	Знает верно и в полном объеме основные методы критического анализа и основы системного подхода как общенаучного метода.	Продвинутый	
				Умеет верно и в полном объеме анализировать задачу, используя основы критического анализа и системного подхода.		
						Умеет верно и в полном объеме осуществлять поиск необходимой для решения поставленной задачи информации, критически оценивая надежность различных источников информации.
		Умеет верно и в полном объеме: использовать современный инструментарий и интеллектуальные информационно-аналитические системы				
		ОПК-2. Способен осуществлять сбор, обработку и статистический анализ данных, необходимых для решения поставленных экономических задач.				ОПК-2.1. Использует основные методы, средства получения, представления, хранения и обработки статистических данных.
			Умеет верно и в полном объеме работать с национальными и международными базами данных с целью поиска информации, необходимой для решения поставленных экономических задач.			
Умеет верно и в полном объеме рассчитывать экономические и социально-экономические показатели, характеризующие деятельность хозяйствующих субъектов на основе типовых методик и действующей						

				нормативно-правовой базы	
				Умеет верно и в полном объеме представить наглядную визуализацию данных.	
				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	
70 – 84 баллов	«зачтено»	ОПК-6. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ОПК-6.2. Понимает принципы работы современных цифровых информационных технологий, соответствующих содержанию профессиональных задач	Умеет верно и в полном объеме: использовать современные цифровые информационные технологии для решения задач профессиональной деятельности	
				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	
				УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	
				УК-1.1. Осуществляет поиск необходимой информации, опираясь на результаты анализа поставленной задачи	
				Знает с незначительными замечаниями основные методы критического анализа и основы системного подхода как общенаучного метода.	Повышенный
				Умеет с незначительными замечаниями анализировать задачу, используя основы критического анализа и системного подхода.	
				Умеет с незначительными замечаниями осуществлять поиск необходимой для решения поставленной задачи информации, критически оценивая надежность различных источников информации.	
				Умеет с незначительными замечаниями: использовать современный инструментарий и интеллектуальные информационно-аналитические системы	
				ОПК-2. Способен осуществлять сбор, обработку и анализ данных, необходимых для решения	
				ОПК-2.1. Определяет источники информации и осуществляет их поиск на основе	
				Знает с незначительными замечаниями: методы сбора информации, способы и вид ее представления, применяя современное программное обеспечение	

		поставленных управленческих задач, с использованием современного инструментария и интеллектуальных информационно-аналитических систем	поставленных целей для решения профессиональных задач	Умеет с незначительными замечаниями: использовать современный инструментарий и интеллектуальные информационно-аналитические системы	
		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	
				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-1.1. Осуществляет поиск необходимой информации, опираясь на результаты анализа поставленной задачи	Знает на базовом уровне с ошибками основные методы критического анализа и основы системного подхода как общенаучного метода.	Базовый
				Умеет с незначительными замечаниями анализировать задачу, используя основы критического анализа и системного подхода.	
				Умеет с незначительными замечаниями осуществлять поиск необходимой для решения поставленной задачи информации, критически оценивая надежность различных источников информации.	
				Умеет с незначительными замечаниями: использовать современный инструментарий и интеллектуальные информационно-аналитические системы	

		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-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 на базовом уровне, с ошибками: характеристики соответствующих содержанию профессиональных задач современных цифровых информационных технологий	
				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-1.1. Осуществляет поиск необходимой информации, опираясь на результаты анализа поставленной задачи	Не знает на базовом уровне основные методы критического анализа и основы системного подхода как общенаучного метода.	Компетенции не сформированы
				Не умеет на базовом уровне анализировать задачу, используя основы критического анализа и системного подхода.	
				Не умеет с на базовом уровне осуществлять поиск необходимой для решения поставленной задачи информации, критически	

				оценивая надежность различных источников информации.	
				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 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	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 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 экономики и цифровых технологий

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ
Б1.О.ДЭ.02.01 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Направление подготовки **38.03.01 ЭКОНОМИКА**

Направленность (профиль) программы
ЭКОНОМИКА И УПРАВЛЕНИЕ НА ПРЕДПРИЯТИИ
(ОРГАНИЗАЦИИ)

Уровень высшего образования **Бакалавриат**

Год начала подготовки - 2026 г.

Краснодар – 2025 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
	<i>Раздел 1. Основные определения и понятия информационной безопасности</i>
1.	Тема 1. Информация как объект защиты. Правовое обеспечение информационной безопасности
2.	Тема 2. Организационное обеспечение информационной безопасности
	<i>Раздел 2. Программно-аппаратные средства и методы обеспечения информационной безопасности</i>
3.	Тема 3. Программно-аппаратные средства обеспечения информационной безопасности в информационных сетях.
4.	Тема 4. Стандарты и спецификации в области информационной безопасности
Трудоемкость дисциплины составляет 3 з.е. / 108 часа.	

Форма контроля – зачет.

Составитель:

к.т.н., доцент кафедры экономики и цифровых технологий Р.Н. Фролов