Приложение 3
к основной профессиональной образовательной программе
по направлению подготовки 09.03.03 «Прикладная информатика»
направленность (профиль) программы «Прикладная информатика в экономике»

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.13 Информационная безопасность

Направление подготовки: **09.03.03 Прикладная информатика**

Направленность (профиль) программы: **Прикладная информатика в экономике**

Уровень высшего образования **Бакалавриат**

Год начала подготовки 2023

Краснодар – 2022 г

Составитель:

к.т.н., доцент кафедры бухгалтерского учета и анализа Р.Н. Фролов

Рабочая программа одобрена на заседании кафедры бухгалтерского учета и анализа Краснодарского филиала РЭУ им. Г.В. Плеханова протокол № 6 от 10 января 2022 г.

Рабочая программа составлена на основе рабочей программы по дисциплине «Информационная безопасность», утвержденной на заседании базовой кафедры Прикладной информатики и информационной безопасности федерального государственного бюджетного образовательного учреждения высшего образования «Российский экономический университета имени Г.В. Плеханова» протокол № 10 от 28 апреля 2021 г., разработанной авторами:
Козыревым П.А., ассистентом, базовой кафедры Прикладной информатики и информационной безопасности
Креопаловым В.В., к.т.н, доцент кафедры прикладной информатики и информационной безопасности

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.

Место дисциплины в структуре образовательной программы

Дисциплина «Информационная безопасность», относится к обязательной части учебного плана.

Объем дисциплины и виды учебной работы

Таблица 1

Показатели объема дисциплины	**Всего часов по формам обучения**	
	очная	***заочная***
Объем дисциплины в зачетных единицах	**4 ЗЕТ**	
Объем дисциплины в часах	**144**	
Промежуточная аттестация: форма	*Экзамен*	*Экзамен*
Контактная работа обучающихся с преподавателем (Контакт. часы), всего:	46	16
1. Контактная работа на проведение занятий лекционного и семинарского типов, всего часов, в том числе:	42	12
• лекции	12	6
• практические занятия	30	6
• лабораторные занятия	-	-
в том числе практическая подготовка	-	-
2. Индивидуальные консультации (ИК)	-	-

3. Контактная работа по промежуточной аттестации (Катт)	-	
4. Консультация перед экзаменом (КЭ)	2	2
5. Контактная работа по промежуточной аттестации в период экз. сессии / сессии заочников (Каттэк)	2	2
Самостоятельная работа (СР), всего:	98	128
в том числе:		
• самостоятельная работа в период экз. сессии (СРэк)	32	5
• самостоятельная работа в семестре (СРс)	66	123
в том числе, самостоятельная работа на курсовую работу	-	-
• изучение ЭОР	-	-
• изучение онлайн-курса или его части	-	-
• выполнение индивидуального проекта	-	-
• подготовка к написанию реферата	-	-

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-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2.1. Понимает базовые принципы постановки задач и выработки решений	УК-2.1. З-1. Знает основные принципы и концепции в области целеполагания и принятия решений УК-2.1. З-2. Знает методы генерирования альтернатив решений и приведения их к сопоставимому виду для выбора оптимального решения УК-2.1. З-3. Знает природу данных, необходимых для решения поставленных задач УК-2.1. У-1. Умеет системно анализировать поставленные цели, формулировать задачи и предлагать обоснованные решения УК-2.1. У-2. Умеет критически оценивать информацию о предметной области принятия решений УК-2.1. У-3. Умеет использовать инструментальные средства для разработки и принятия решений
	УК-2.2. Выбирает оптимальные способы решения задач, исходя из действующих правовых	УК-2.2. З-1. Знает основные методы принятия решений, в том числе в условиях риска и неопределенности УК-2.2. З-2. Знает виды и источники

	норм, имеющихся ресурсов и ограничений	возникновения рисков принятия решений, методы управления ими УК-2.2. З-3. Знает основные нормативно-правовые документы, регламентирующие процесс принятия решений в конкретной предметной области УК-2.2. У-1. Умеет проводить многофакторный анализ элементов предметной области для выявления ограничений при принятии решений УК-2.2. У-2. Умеет разрабатывать и оценивать альтернативные решения с учетом рисков УК-2.2. У-3. Умеет выбирать оптимальные решения исходя из действующих правовых норм, имеющихся ресурсов и ограничений
ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3.2. Решает задачи профессиональной деятельности с учетом основных требований информационной безопасности	ОПК-3.2. З-1. Знает методологические и технологические основы комплексного обеспечения безопасности автоматизированных информационных систем ОПК-3.2. З-2. Знает методы и средства, современные подходы к построению систем защиты информации, критерии оценки защищенности ИС, принципы формирования политики информационной безопасности в автоматизированных системах ОПК-3.2. З-3. Знает нормативно-правовые документы по обеспечению информационной безопасности, стандарты построения систем информационной безопасности и оценки степени защиты систем информационной безопасности объектов ОПК-3.2. З-4. Знает основные методы контроля эффективности обеспечения информационной безопасности информационных систем ОПК-3.2. У-1. Умеет разрабатывать модели угроз и нарушителей информационной безопасности ИС, выявлять угрозы информационной безопасности и обосновывать организационно-технические мероприятия по защите информации в ИС

		ОПК-3.2. У-2. Умеет выявлять уязвимости информационно-технологических ресурсов автоматизированных систем и проводить мониторинг угроз безопасности ИС ОПК-3.2. У-3. Умеет анализировать риски информационных систем, осуществлять оценку защищенности и обеспечения информационной безопасности информационных систем ОПК-3.2. У-4. Умеет выполнять работы на стадиях и этапах создания ИС в защищенном исполнении ОПК-3.2. У-5. Умеет составлять аналитические обзоры по вопросам обеспечения информационной безопасности ИС и разрабатывать частные политики информационной безопасности ИС

II. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

этапы формирования и критерии оценивания сформированности компетенций 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 курсу в целом)
		Лекции	Практические занятия	Лабораторные занятия	Практическая подготовка	Самостоятельная работа/ КЭ, Каттэк, Катт	Всего					
	Семестр 6											
1.	**Тема 1. Стандарты и нормативно-правовые акты в области информационной безопасности.** Системный подход к проектированию, внедрению и поддержанию системы обеспечения ИБ на предприятии. Стандартизация в сфере управления информационной безопасностью (на основе международных стандартов ISO/IEC 17799, ISO/IEC 27002, ISO/IEC 27001, ISO/IEC 15408). Ресурсы предприятия, подлежащие защите с точки зрения ИБ. Отечественные и международные стандарты в области защиты информации. Стандарты в области разработки и внедрения программного обеспечения и автоматизированных систем. Аспекты ИБ в рамках менеджмента непрерывности бизнеса. Соответствие требованиям законодательства. Соответствие политикам безопасности и стандартам, техническое соответствие. Создание удостоверяющего центра, генерация открытых и ключей, создание сертификатов открытых ключей, создание электронной подписи.	4	10	-		20	34	УК-2.1. УК-2.2. ОПК-3.2.	УК-2.1. З-1. УК-2.1. З-2. УК-2.1. У-2. УК-2.1. У-3. УК-2.2. З-1. УК-2.2. У-1. УК-2.2. У-2. УК-2.2. У-3. ОПК-3.2. З-1. ОПК-3.2. З-2. ОПК-3.2. З-4. ОПК-3.2. У-1. ОПК-3.2. У-5.	Пр.з.	Т.	-

2.	**Тема 2. Анализ рисков и угроз 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. Анализ ошибок, уничтожение, неавторизованная модификация или нецелевое использование информации в прикладных программах. Криптографические меры и средства контроля и управления. Безопасность системных файлов. Безопасность в процессах разработки и поддержки. 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.	4	10	-		20	34	УК-2.1. УК-2.2. ОПК-3.2.	УК-2.1. З-1. УК-2.1. У-1. УК-2.1. У-2. УК-2.1. У-3. УК-2.2. З-1. УК-2.2. З-2. УК-2.2. У-1. ОПК-3.2. З-1. ОПК-3.2. З-2. ОПК-3.2. З-3. ОПК-3.2. З-4. ОПК-3.2. У-3. ОПК-3.2. У-4. ОПК-3.2. У-5.	Пр.з.	К/р	-

3.	**Тема 3. Проектирование, разработка и внедрение автоматизированных систем в защищенном исполнении.** 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. Техническое задание на создание автоматизированной системы. Порядок создания автоматизированных систем в защищенном исполнении. Требования к разработке и внедрению автоматизированной системы в защищенном исполнении. Безопасность информации и средств обработки информации защищенных ИС при доступе, обработке, передаче и менеджменте, осуществляемом сторонними организациями. Защита информационных активов защищенных ИС. Анализ и классификация информации, циркулирующей в защищенных ИС. Разработка требований безопасности защищенных ИС.	4	10	-		26	40	УК-2.1. УК-2.2. ОПК-3.2.	УК-2.1. З-1. УК-2.1. З-2. УК-2.1. З-3. УК-2.2. З-3. УК-2.2. У-1. УК-2.2. У-2. УК-2.2. У-3. ОПК-3.2. З-1. ОПК-3.2. З-2. ОПК-3.2. З-3. ОПК-3.2. У-2. ОПК-3.2. У-3. ОПК-3.2. У-4. ОПК-3.2. У-5.	Пр.з.	К/р	Р.
	Консультация перед экзаменом (КЭ)	-	-	-	-	-/2	2	-	-	-	-	-
	Контактная работа по промежуточной аттестации в период экз. сессии / сессии заочников (Каттэк)	-	-	-	-	-/2	2	-	-	-	-	-
	Самостоятельная работа в период экз. сессии (СРэк)	-	-	-	-	32/-	32	-	-	-	-	-
	Итого	12	30	-	-	98/4	144	x	x	x	x	x

этапы формирования и критерии оценивания сформированности компетенций обучающихся 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 5											
1.	**Тема 1. Стандарты и нормативно-правовые акты в области информационной безопасности.** Системный подход к проектированию, внедрению и поддержанию системы обеспечения ИБ на предприятии. Стандартизация в сфере управления информационной безопасностью (на основе международных стандартов ISO/IEC 17799, ISO/IEC 27002, ISO/IEC 27001, ISO/IEC 15408). Ресурсы предприятия, подлежащие защите с точки зрения ИБ. Отечественные и международные стандарты в области защиты информации. Стандарты в области разработки и внедрения программного обеспечения и автоматизированных систем. Аспекты ИБ в рамках менеджмента непрерывности бизнеса. Соответствие требованиям законодательства. Соответствие политикам безопасности и стандартам, техническое соответствие. Создание удостоверяющего центра, генерация открытых и ключей, создание сертификатов открытых ключей, создание электронной подписи.	2	2	-		41	45	УК-2.1. УК-2.2. ОПК-3.2.	УК-2.1. З-1. УК-2.1. З-2. УК-2.1. У-2. УК-2.1. У-3. УК-2.2. З-1. УК-2.2. У-1. УК-2.2. У-2. УК-2.2. У-3. ОПК-3.2. З-1. ОПК-3.2. З-2. ОПК-3.2. З-4. ОПК-3.2. У-1. ОПК-3.2. У-5.	Пр.з.	Т.	-

2.	**Тема 2. Анализ рисков и угроз 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. Анализ ошибок, уничтожение, неавторизованная модификация или нецелевое использование информации в прикладных программах. Криптографические меры и средства контроля и управления. Безопасность системных файлов. Безопасность в процессах разработки и поддержки. 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	-		41	45	УК-2.1. УК-2.2. ОПК-3.2.	УК-2.1. З-1. УК-2.1. У-1. УК-2.1. У-2. УК-2.1. У-3. УК-2.2. З-1. УК-2.2. З-2. УК-2.2. У-1. ОПК-3.2. З-1. ОПК-3.2. З-2. ОПК-3.2. З-3. ОПК-3.2. З-4. ОПК-3.2. У-3. ОПК-3.2. У-4. ОПК-3.2. У-5.	Пр.з.	К/р	-

3.	**Тема 3. Проектирование, разработка и внедрение автоматизированных систем в защищенном исполнении.** 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. Техническое задание на создание автоматизированной системы. Порядок создания автоматизированных систем в защищенном исполнении. Требования к разработке и внедрению автоматизированной системы в защищенном исполнении. Безопасность информации и средств обработки информации защищенных ИС при доступе, обработке, передаче и менеджменте, осуществляемом сторонними организациями. Защита информационных активов защищенных ИС. Анализ и классификация информации, циркулирующей в защищенных ИС. Разработка требований безопасности защищенных ИС.	2	2	-		41	45	УК-2.1. УК-2.2. ОПК-3.2.	УК-2.1. З-1. УК-2.1. З-2. УК-2.1. З-3. УК-2.2. З-3. УК-2.2. У-1. УК-2.2. У-2. УК-2.2. У-3. ОПК-3.2. З-1. ОПК-3.2. З-2. ОПК-3.2. З-3. ОПК-3.2. У-2. ОПК-3.2. У-3. ОПК-3.2. У-4. ОПК-3.2. У-5.	Пр.з.	К/р	Р.
	Консультация перед экзаменом (КЭ)	-	-	-	-	-/2	2	-	-	-	-	-
	Контактная работа по промежуточной аттестации в период экз. сессии / сессии заочников (Каттэк)	-	-	-	-	-/2	2	-	-	-	-	-
	Самостоятельная работа в период экз. сессии (СРэк)	-	-	-	-	5/-	5	-	-	-	-	-
	Итого	6	6	-	-	128/4	144	x	x	x	x	x

Формы учебных заданий на аудиторных занятиях:

Практическая задания (Пр.з.)

Формы текущего контроля:

Контрольные работы (К/р)

Тест (Т.)

Формы заданий для творческого рейтинга:

Реферат (Р.)

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). — 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

Нормативные правовые документы:

1. Федеральный закон Российской Федерации от 27 июля 2006 г. N 149-ФЗ Об информации, информационных технологиях и о защите информации
2. 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/
3. "Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы" [Электрон. ресурс]. – Режим доступа http://www.consultant.ru/document/cons_doc_LAW_216363
4. Постановление Правительства РФ от 26.06.1995 О сертификации средств защиты информации N 608
5. Постановление Правительства РФ от 15 августа 2006 г. N 504 О лицензировании деятельности по технической защите конфиденциальной информации
6. Постановление Правительства РФ от 31 августа 2006 г. N 532 О лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации

7. Приказ ФСБ РФ от 9 февраля 2005 г. N 66 "Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)"
8. Постановление Правительства Российской Федерации от 17 ноября 2007 г. N 781 г. Москва "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных"

ПЕРЕЧЕНЬ ИНФОРМАЦИОННО-СПРАВОЧНЫХ СИСТЕМ

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

ПЕРЕЧЕНЬ ЭЛЕКТРОННО-ОБРАЗОВАТЕЛЬНЫХ РЕСУРСОВ

1. Курс "Информационная безопасность" (электронный образовательный ресурс, размещён в ЭОС РЭУ им. Г.В. Плеханова) http://lms.rea.ru

ПЕРЕЧЕНЬ ПРОФЕССИОНАЛЬНЫХ БАЗ ДАННЫХ

1. http://www.anti-malware.ru/ — независимый информационно-аналитический портал по безопасности

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

1. http://www.fsb.ru/ (сайт ФСБ России);
2. http://www.infoforum.ru/ Национальный форум информационной безопасности "ИНФОФОРУМ" — электронное периодическое издание по вопросам информационной безопасности
3. http://www.komitet2-16.km.duma.gov.ru/ (сайт комитета Государственной Думы по безопасности);
4. http://www.scrf.gov.ru/ (сайт Совета безопасности Российской Федерации);

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

Лицензионное программное обеспечение:

- Операционная система Windows 10,
Microsoft Office Professional Plus: 2019 год (MS Word, MS Excel, MS Power Point, MS Access)
- Антивирусная программа Касперского Kaspersky Endpoint Securrity для бизнеса Расширенный Rus Edition

МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Дисциплина «Информационная безопасность» 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.

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 «**Информационная безопасность**» 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 (*экзамен*)	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 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 «Информационная безопасность» учебным планом не предусмотрена

Вопросы к экзамену:

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.
62. Сущность криптографических методов.
63. Организационно-административные мероприятия обеспечения компьютерной безопасности.
64. Организация конфиденциального делопроизводства.
65. Принципы обеспечения информационную безопасности на основе инженерно-технического обеспечения.
66. Типы и субъекты информационных угроз.

Практические задания к экзамену

1. Британский стандарт BS 7799.
2. Британский стандарт BS 7799 – 1.
3. Британский стандарт BS 7799 – 2.
4. Британский стандарт BS 7799 – 3.
5. Международный стандарт ISO/IEC 17799.
6. Семейство Международных стандартов ISO/IEC 27000.
7. Международный стандарт ISO/IEC 27001.
8. Международный стандарт ISO/IEC 27002.
9. Национальный стандарт ГОСТ Р 50922.
10. Национальный стандарт Р 50.1.053.
11. Национальный стандарт ГОСТ Р 51188.
12. Национальный стандарт ГОСТ Р 51275.
13. Национальный стандарт ГОСТ Р ИСО/МЭК 15408.
14. Национальный стандарт ГОСТ Р ИСО/МЭК 15408-1.
15. Национальный стандарт ГОСТ Р ИСО/МЭК 15408-2.
16. Национальный стандарт ГОСТ Р ИСО/МЭК 15408-3.
17. Национальный стандарт ГОСТ Р ИСО/МЭК 17799.
18. Национальный стандарт ГОСТ Р ИСО/МЭК 27001.
19. Назначение, структура и методика построения разрешительной системы доступа персонала к

секретам фирмы.

20. Порядок проведения переговоров и совещаний по конфиденциальным вопросам.
21. Виды и назначение технических средств защиты информации в помещениях, используемых для ведения переговоров и совещаний.
22. Порядок работы с посетителями фирмы, организационные и технические методы защиты секретов фирмы.
23. Порядок защиты информации в рекламной и выставочной деятельности.
24. Организационное обеспечение защиты информации, обрабатываемой средствами вычислительной и организационной техники.

Тестовые задания

1. Какое семейство (стек) протоколов наиболее распространено в сфере межсетевого взаимодействия?

1. TCP/IP
2. TCP/UDP
3. IP/UDP
4. FTP/UDP

2. Любая характеристика, использование которой нарушителем может привести к реализации угрозы

1. Уязвимость
2. Риск
3. Угроза
4. Критический параметр

3. Потенциально возможное событие, действие, процесс или явление, которое может вызвать нанесение ущерба (материального, морального или иного) ресурсам системы

1. Угроза
2. Уязвимость
3. Риск
4. Критический параметр

4. Нарушение работоспособности элемента системы, приводящее к невозможности выполнения им основных своих функций

1. Отказ
2. Сбой
3. Ошибка
4. Побочное влияние

5. Временное нарушение работоспособности элемента системы, следствием чего может быть неправильное выполнение им в этот момент своей функции

1. Сбой
2. Ошибка
3. Отказ
4. Побочное влияние

6. Неправильное выполнение элементом одной или нескольких функций, происходящее вследствие специфического его состояния

1. Ошибка
2. Сбой

3. Отказ
4. Побочное влияние

Задания для контрольных работ

1. Провести оценку рисков информационной безопасности для предложенной организации.
2. Составить техническое задание на разработку автоматизированной системы в защищенном исполнении.
3. Дать определение информационной безопасности.
4. Какие виды компьютерных преступлений существуют?
5. Какие виды злоумышленников существуют?
6. Методология построения и оценки СЗИ.
7. Дайте определение угрозы, актива, атаки, уязвимости. Обоснуйте их взаимосвязь.

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.

Структура экзаменационного билета

Наименование оценочного средства	***Максимальное количество баллов***
Вопрос 1	*14*
Вопрос 2	*14*
Практическое задание	*12*

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	**«отлично»**	**УК-2.** Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений. **ОПК-3.** Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**УК-2.1.** Понимает базовые принципы постановки задач и выработки решений. **УК-2.2.** Выбирает оптимальные способы решения задач, исходя из действующих правовых норм, имеющихся ресурсов и ограничений. **ОПК-3.2.** Решает задачи профессиональной деятельности с учетом основных требований информационной безопасности	**Знает верно и в полном объеме:** основные принципы и концепции в области целеполагания и принятия решений; методы генерирования альтернатив решений и приведения их к сопоставимому виду для выбора оптимального решения; природу данных, необходимых для решения поставленных задач; основные методы принятия решений, в том числе в условиях риска и неопределенности; виды и источники возникновения рисков принятия решений, методы управления ими; основные нормативно-правовые документы, регламентирующие процесс принятия решений в конкретной предметной области; методологические и технологические основы комплексного обеспечения безопасности автоматизированных информационных систем; методы и средства, современные подходы к построению систем защиты информации, критерии оценки защищенности ИС, принципы формирования политики информационной безопасности в автоматизированных системах; нормативно-правовые документы по обеспечению информационной безопасности, стандарты построения систем информационной безопасности и оценки степени защиты систем информационной безопасности объектов; основные методы контроля эффективности обеспечения информационной безопасности информационных систем. **Умеет верно и в полном объеме:** системно анализировать поставленные цели, формулировать задачи и предлагать обоснованные решения; критически оценивать информацию о предметной области принятия решений; использовать инструментальные средства для разработки и принятия решений; проводить многофакторный анализ элементов предметной области для выявления ограничений при принятии решений; разрабатывать и	**Продвинутый**

				оценивать альтернативные решения с учетом рисков; выбирать оптимальные решения исходя из действующих правовых норм, имеющихся ресурсов и ограничений; разрабатывать модели угроз и нарушителей информационной безопасности ИС, выявлять угрозы информационной безопасности и обосновывать организационно-технические мероприятия по защите информации в ИС; выявлять уязвимости информационно-технологических ресурсов автоматизированных систем и проводить мониторинг угроз безопасности ИС; анализировать риски информационных систем, осуществлять оценку защищенности и обеспечения информационной безопасности информационных систем; выполнять работы на стадиях и этапах создания ИС в защищенном исполнении; составлять аналитические обзоры по вопросам обеспечения информационной безопасности ИС и разрабатывать частные политики информационной безопасности ИС.	
70 – 84 баллов	**«хорошо»**	**УК-2.** Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений. **ОПК-3.** Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**УК-2.1.** Понимает базовые принципы постановки задач и выработки решений. **УК-2.2.** Выбирает оптимальные способы решения задач, исходя из действующих правовых норм, имеющихся ресурсов и ограничений. **ОПК-3.2.** Решает задачи профессиональной деятельности с учетом основных требований информационной безопасности	**Знает с незначительными замечаниями:** основные принципы и концепции в области целеполагания и принятия решений; методы генерирования альтернатив решений и приведения их к сопоставимому виду для выбора оптимального решения; природу данных, необходимых для решения поставленных задач; основные методы принятия решений, в том числе в условиях риска и неопределенности; виды и источники возникновения рисков принятия решений, методы управления ими; основные нормативно-правовые документы, регламентирующие процесс принятия решений в конкретной предметной области; методологические и технологические основы комплексного обеспечения безопасности автоматизированных информационных систем; методы и средства, современные подходы к построению систем защиты информации, критерии оценки защищенности ИС, принципы формирования политики информационной безопасности в автоматизированных системах; нормативно-правовые документы по обеспечению информационной безопасности, стандарты построения	**Повышенный**

				систем информационной безопасности и оценки степени защиты систем информационной безопасности объектов; основные методы контроля эффективности обеспечения информационной безопасности информационных систем. **Умеет с незначительными замечаниями:** системно анализировать поставленные цели, формулировать задачи и предлагать обоснованные решения; критически оценивать информацию о предметной области принятия решений; использовать инструментальные средства для разработки и принятия решений; проводить многофакторный анализ элементов предметной области для выявления ограничений при принятии решений; разрабатывать и оценивать альтернативные решения с учетом рисков; выбирать оптимальные решения исходя из действующих правовых норм, имеющихся ресурсов и ограничений; разрабатывать модели угроз и нарушителей информационной безопасности ИС, выявлять угрозы информационной безопасности и обосновывать организационно-технические мероприятия по защите информации в ИС; выявлять уязвимости информационно-технологических ресурсов автоматизированных систем и проводить мониторинг угроз безопасности ИС; анализировать риски информационных систем, осуществлять оценку защищенности и обеспечения информационной безопасности информационных систем; выполнять работы на стадиях и этапах создания ИС в защищенном исполнении; составлять аналитические обзоры по вопросам обеспечения информационной безопасности ИС и разрабатывать частные политики информационной безопасности ИС.	
50 – 69 баллов	**«удовлетворительно»**	**УК-2.** Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и	**УК-2.1.** Понимает базовые принципы постановки задач и выработки решений. **УК-2.2.** Выбирает оптимальные способы	**Знает на базовом уровне, с ошибками:** основные принципы и концепции в области целеполагания и принятия решений; методы генерирования альтернатив решений и приведения их к сопоставимому виду для выбора оптимального решения; природу данных, необходимых для решения поставленных задач; основные методы принятия решений, в том числе в условиях риска и	**Базовый**

		ограничений. **ОПК-3.** Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	решения задач, исходя из действующих правовых норм, имеющихся ресурсов и ограничений. **ОПК-3.2.** Решает задачи профессиональной деятельности с учетом основных требований информационной безопасности	неопределенности; виды и источники возникновения рисков принятия решений, методы управления ими; основные нормативно-правовые документы, регламентирующие процесс принятия решений в конкретной предметной области; методологические и технологические основы комплексного обеспечения безопасности автоматизированных информационных систем; методы и средства, современные подходы к построению систем защиты информации, критерии оценки защищенности ИС, принципы формирования политики информационной безопасности в автоматизированных системах; нормативно-правовые документы по обеспечению информационной безопасности, стандарты построения систем информационной безопасности и оценки степени защиты систем информационной безопасности объектов; основные методы контроля эффективности обеспечения информационной безопасности информационных систем. **Умеет на базовом уровне, с ошибками:** системно анализировать поставленные цели, формулировать задачи и предлагать обоснованные решения; критически оценивать информацию о предметной области принятия решений; использовать инструментальные средства для разработки и принятия решений; проводить многофакторный анализ элементов предметной области для выявления ограничений при принятии решений; разрабатывать и оценивать альтернативные решения с учетом рисков; выбирать оптимальные решения исходя из действующих правовых норм, имеющихся ресурсов и ограничений; разрабатывать модели угроз и нарушителей информационной безопасности ИС, выявлять угрозы информационной безопасности и обосновывать организационно-технические мероприятия по защите информации в ИС; выявлять уязвимости информационно-технологических ресурсов автоматизированных систем и проводить мониторинг угроз безопасности ИС; анализировать риски информационных систем, осуществлять оценку защищенности и обеспечения информационной	

				безопасности информационных систем; выполнять работы на стадиях и этапах создания ИС в защищенном исполнении; составлять аналитические обзоры по вопросам обеспечения информационной безопасности ИС и разрабатывать частные политики информационной безопасности ИС.	
менее 50 баллов	**«неудовлетворительно»**	**УК-2.** Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений. **ОПК-3.** Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**УК-2.1.** Понимает базовые принципы постановки задач и выработки решений. **УК-2.2.** Выбирает оптимальные способы решения задач, исходя из действующих правовых норм, имеющихся ресурсов и ограничений. **ОПК-3.2.** Решает задачи профессиональной деятельности с учетом основных требований информационной безопасности	**Не знает на базовом уровне:** основные принципы и концепции в области целеполагания и принятия решений; методы генерирования альтернатив решений и приведения их к сопоставимому виду для выбора оптимального решения; природу данных, необходимых для решения поставленных задач; основные методы принятия решений, в том числе в условиях риска и неопределенности; виды и источники возникновения рисков принятия решений, методы управления ими; основные нормативно-правовые документы, регламентирующие процесс принятия решений в конкретной предметной области; методологические и технологические основы комплексного обеспечения безопасности автоматизированных информационных систем; методы и средства, современные подходы к построению систем защиты информации, критерии оценки защищенности ИС, принципы формирования политики информационной безопасности в автоматизированных системах; нормативно-правовые документы по обеспечению информационной безопасности, стандарты построения систем информационной безопасности и оценки степени защиты систем информационной безопасности объектов; основные методы контроля эффективности обеспечения информационной безопасности информационных систем. **Не умеет на базовом уровне:** системно анализировать поставленные цели, формулировать задачи и предлагать обоснованные решения; критически оценивать информацию о предметной области принятия решений; использовать инструментальные средства для разработки и принятия решений; проводить многофакторный анализ элементов предметной области для выявления ограничений при принятии решений; разрабатывать и	**Компетенции не сформированы**

				оценивать альтернативные решения с учетом рисков; выбирать оптимальные решения исходя из действующих правовых норм, имеющихся ресурсов и ограничений; разрабатывать модели угроз и нарушителей информационной безопасности ИС, выявлять угрозы информационной безопасности и обосновывать организационно-технические мероприятия по защите информации в ИС; выявлять уязвимости информационно-технологических ресурсов автоматизированных систем и проводить мониторинг угроз безопасности ИС; анализировать риски информационных систем, осуществлять оценку защищенности и обеспечения информационной безопасности информационных систем; выполнять работы на стадиях и этапах создания ИС в защищенном исполнении; составлять аналитические обзоры по вопросам обеспечения информационной безопасности ИС и разрабатывать частные политики информационной безопасности ИС.	

Министерство науки и высшего образования Российской Федерации

федеральное государственное бюджетное образовательное учреждение высшего образования
«Российский экономический университет имени Г.В. Плеханова»

Факультет экономики, менеджмента и торговли

Кафедра бухгалтерского учета и анализа

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

Б1.О.13 Информационная безопасность

Направление подготовки: **09.03.03 Прикладная информатика**

Направленность (профиль) программы: **Прикладная информатика в экономике**

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
1.	Тема 1. Стандарты и нормативно-правовые акты в области информационной безопасности.
2.	Тема 2. Анализ рисков и угроз информационной безопасности.
3.	Тема 3. Проектирование, разработка и внедрение автоматизированных систем в защищенном исполнении.
Трудоемкость дисциплины составляет 4 з.е. / 144 часов.	

Форма контроля – *экзамен*

Составители:
ассистент кафедры прикладной информатики и информационной безопасности П.А. Козырев
к.т.н, доцент кафедры прикладной информатики и информационной безопасности В.В. Креопалов
к.т.н., доцент кафедры бухгалтерского учета и анализа Р.Н. Фролов