Приложение 3
к основной профессиональной образовательной программе
по направлению подготовки
38.03.6 Торговое дело
направленность (профиль) программы Торговый менеджмент
и маркетинг (во внутренней и внешней торговле)

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 торгового дела

Кафедра бухгалтерского учета и анализа

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.О.ДЭ.02.02 Основы информационной безопасности

Направление подготовки 38.03.06 Торговое дело

направление (профиль) программы
Торговый менеджмент и маркетинг (во внутренней и внешней торговли)

Уровень высшего образования ***Бакалавриат***

Год начала подготовки 2022

Краснодар – 2021 г.

Составитель:
к.п.н., доцент кафедры бухгалтерского
учета и анализа В.В. Салий

Рабочая программа одобрена на заседании кафедры
Бухгалтерского учета и анализа
протокол № 1 от «30» августа 2021 г.

СОДЕРЖАНИЕ

I. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ

Цель и задачи освоения дисциплины

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

Задачи дисциплины:

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

2.Содержание дисциплины:

Место дисциплины в структуре образовательной программы

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

Объем дисциплины и виды учебной работы

Таблица 1

Показатели объема дисциплины *	**Всего часов по формам обучения**	
	очная	***очно-заочная****
Объем дисциплины в зачетных единицах	***3 ЗЕТ***	
Объем дисциплины в акад.часах	***108***	
Промежуточная аттестация: форма	зачет	зачет
Контактная работа обучающихся с преподавателем (Контакт.часы), всего:	30	14
1. Аудиторная работа (Ауд.), акад. часов всего, в том числе:	28	*12*
• лекции	*12*	*6*

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

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. З-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.

II. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

этапы формированияи критерии оценивания сформированности компетенций

для студентов **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, Кост	Всего					
	Семестр 4											
	Раздел 1. Основные определения и понятия информационной безопасности											
1.	**Тема 1. Информация как объект защиты. Правовое обеспечение информационной безопасности** Информационная безопасность. Основные понятия. Модели информационной безопасности. Виды защищаемой информации. Основные нормативно-правовые акты в области информационной безопасности. Правовые особенности обеспечения безопасности конфиденциальной информации и государственной тайны. Ресурсы предприятия, подлежащие защите с точки зрения ИБ. Аспекты ИБ в рамках менеджмента непрерывности бизнеса.	*2*	4			***18/-***	24	*УК-1.1.*	*УК-1.1. З-1. УК-1.1. У-1. УК-1.1.У-2*	О.		-

2.	**Тема 2. Организационное обеспечение информационной безопасности** Основные стандарты в области обеспечения информационной безопасности. Политика безопасности. Экономическая безопасность предприятия. Инженерная защита объектов. Защита информации от утечки по техническим каналам. Использование баз данных для нахождения и изучения нормативных документов в области информационной безопасности. Идентификация и оценка активов. Модель угроз. Идентификация уязвимостей. Оценка рисков. Обработка рисков. Модель нарушителя политики безопасности. Типичные угрозы информации и уязвимости корпоративных информационных систем.	*4*	4			***18/-***	26	*УК-1.1.*	*УК-1.1. З-1.* *УК-1.1. У-1.* *УК-1.1.У-2*	О.	К.	Д.
Раздел 2. Программно-аппаратные средства и методы обеспечения информационной безопасности												
3.	**Тема 3. Программно-аппаратные средства обеспечения информационной безопасности в информационных сетях** Основные виды сетевых и компьютерных угроз. Средства и методы защиты от сетевых компьютерных угроз. Симметричные и ассиметричные системы шифрования. Цифровые подписи (Электронные подписи). Инфраструктура открытых ключей. Криптографические протоколы.	*2*	***4***			***21/-***	27	*УК-1.1.*	*УК-1.1. З-1.* *УК-1.1. У-1.* *УК-1.1.У-2*	Гр.д.	К.	Ан.О.

4.	**Тема 4. Стандарты и спецификации в области информационной безопасности** Стандартизация в сфере управления информационной безопасностью (на основе международных стандартов ISO/IEC 17799, ISO/IEC27002, ISO/IEC27001,ISO/IEC 15408). Создание зашифрованных файлов и криптоконтейнеров и их расшифрование. Соответствие требованиям законодательства. Соответствие политикам безопасности и стандартам, техническое соответствие. Создание удостоверяющего центра, генерация открытых и секретных ключей, создание сертификатов открытых ключей, создание электронной подписи, проверка электронной подписи.	*4*	***4***			***21/-***	29	*УК-1.1.*	*УК-1.1. З-1. УК-1.1. У-1. УК-1.1.У-2*	О.	К.р.	
	Контактная работа по промежуточной аттестации (Катт)	-	-	-	-	-/2	2	-	-	-	-	-
	Итого	12	16		2	78/2	108	х	**х**	**х**	**х**	**х**

для студентов очно- за**очной формы обучения** Таблица 3.2

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

1.	**Тема 1. Информация как объект защиты. Правовое обеспечение информационной безопасности** Информационная безопасность. Основные понятия. Модели информационной безопасности. Виды защищаемой информации. Основные нормативно-правовые акты в области информационной безопасности. Правовые особенности обеспечения безопасности конфиденциальной информации и государственной тайны. Ресурсы предприятия, подлежащие защите с точки зрения ИБ. Аспекты ИБ в рамках менеджмента непрерывности бизнеса.	*1*	1			***16/-***	18	*УК-1.1.*	*УК-1.1. З-1. УК-1.1. У-1. УК-1.1.У-2*	О.		-
2.	**Тема 2. Организационное обеспечение информационной безопасности** Основные стандарты в области обеспечения информационной безопасности. Политика безопасности. Экономическая безопасность предприятия. Инженерная защита объектов. Защита информации от утечки по техническим каналам. Использование баз данных для нахождения и изучения нормативных документов в области информационной безопасности. Идентификация и оценка активов. Модель угроз. Идентификация уязвимостей. Оценка рисков. Обработка рисков. Модель нарушителя политики безопасности. Типичные угрозы информации и уязвимости корпоративных информационных систем.	*1*	1			***16/-***	18	*УК-1.1.*	*УК-1.1. З-1. УК-1.1. У-1. УК-1.1.У-2*	О.	К.	Д.
Раздел 2. Программно-аппаратные средства и методы обеспечения информационной безопасности												

3.	**Тема 3. Программно-аппаратные средства обеспечения информационной безопасности в информационных сетях** Основные виды сетевых и компьютерных угроз. Средства и методы защиты от сетевых компьютерных угроз. Симметричные и ассиметричные системы шифрования. Цифровые подписи (Электронные подписи). Инфраструктура открытых ключей. Криптографические протоколы.	*2*	***2***			***30/-***	34	*УК-1.1.*	*УК-1.1. З-1. УК-1.1. У-1. УК-1.1.У-2*	Гр.д.	К.	Ан.О.
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***			***32/-***	36	*УК-1.1.*	*УК-1.1. З-1. УК-1.1. У-1. УК-1.1.У-2*	О.	К.р.	
	Контактная работа по промежуточной аттестации (Катт)	-	-	-	-	-/2	2	-	-	-	-	-
	Итого	6	6		2	94/2	108	х	**х**	**х**	**х**	**х**

III. УЧЕБНО-МЕТОДИЧЕСКОЕ И МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

Основная литература

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

Дополнительная литература:

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

Нормативные правовые документы:

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

ПЕРЕЧЕНЬ ИНФОРМАЦИОННО-СПРАВОЧНЫХ СИСТЕМ

1. Справочно - правовая система «Консультант Плюс»
2. Справочно - правовая система «Гарант»

ПЕРЕЧЕНЬ ПРОФЕССИОНАЛЬНЫХ БАЗ ДАННЫХ

1. http://www.iep.ru/ru/publikatcii/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

1. Операционная система Microsoft Windows 8.1; Microsoft Windows 10
2. Пакет офисных программ Microsoft Office Professional Plus 2010 Rus в составе: Microsoft Word, Microsoft Excel, Microsoft Power Point, Microsoft Access
3. Антивирусная программа «Kaspersky Endpoint Security» для бизнеса
4. Файловый архиватор «7Zip»
5. Приложение для просмотра PDF файлов «Acrobat Adobe Reader»
6. Системы электронного обучения и тестирования: Indigo, Moodle

МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Дисциплина «Основы информационной безопасности» обеспечена:

для проведения занятий лекционного типа:

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

для проведения занятий семинарского типа (практические занятия);

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

IV. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

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

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

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

Таблица 4

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

В соответствии с Положением о рейтинговой системе оценки успеваемости и качества знаний обучающихся «преподаватель кафедры, непосредственно ведущий занятия со студенческой группой, обязан

проинформировать группу о распределении рейтинговых баллов по всем видам работ на первом занятии учебного модуля (семестра), количестве модулей по учебной дисциплине, сроках и формах контроля их освоения, форме промежуточной аттестации, снижении баллов за несвоевременное выполнение выданных заданий. Обучающиеся в течение учебного модуля (семестра) получают информацию о текущем количестве набранных по дисциплине баллов через личный кабинет студента».

VI. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГОКОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ[1]

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

Тематика курсовых работ/проектов

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

Перечень вопросов к зачету:

1. Цели государства в области обеспечения информационной безопасности.
2. Основные нормативные акты РФ, связанные с правовой защитой информации.
3. Виды компьютерных преступлений.
4. Способы и механизмы совершения информационных компьютерных преступлений.
5. Основные параметры и черты информационной компьютерной преступности в России.
6. Компьютерный вирус. Основные виды компьютерных вирусов.
7. Методы защиты от компьютерных вирусов.
8. Типы антивирусных программ.
9. Защиты от несанкционированного доступа. Идентификация и аутентификация пользователя.
10. Основные угрозы компьютерной безопасности при работе в сети Интернет.
11. Виды защищаемой информации.
12. Государственная тайна как особый вид защищаемой информации.
13. Конфиденциальная информация.
14. Система защиты государственной тайны.
15. Правовой режим защиты государственной тайны.

[1]В данном разделе приводятся примеры оценочных средств

16. Защита интеллектуальной собственности средствами патентного и авторского права.
17. Международное законодательство в области защиты информации.
18. Программно-аппаратные средства обеспечения информационной безопасности в информационных сетях.
19. Симметричные шифры.
20. Ассиметричные шифры.
21. Криптографические протоколы.
22. Криптографические хеш-функции.
23. Электронная подпись.
24. Организационное обеспечение информационной безопасности.
25. Служба безопасности организации.
26. Методы защиты информации от утечки в технических каналах.
27. Инженерная защита и охрана объектов.

Типовые тестовые задания:

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

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

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

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

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

Примеры вопросов для опроса:

1. Что такое информационная безопасность?
2. Перечислите основные угрозы информационной безопасности.
3. Какие существуют модели и методы информационной безопасности?
4. Что такое правовые методы защиты информации?
5. Что такое организационные методы защиты информации?

Примеры тем групповых дискуссий:

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

2 Порядок проведения переговоров и совещаний по конфиденциальным вопросам.

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

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

5. Порядок защиты информации в рекламной и выставочной деятельности.

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

Примеры типовых заданий для контрольной работы:

Тема 1. Угрозы информационной безопасности в сетях организации
Для выбранного объекта защиты информации (например, почтовый сервер, компьютер в бухгалтерии, телефонная база ограниченного пользования на электронных носителях и др) провести анализ защищенности объекта по следующим пунктам вид угроз, характер происхождения угроз, классы каналов несанкционированного получения информации, источники появления угроз, причины нарушения целостности информации, потенциально возможные злоумышленные действия. Определить класс защиты информации.

Тема 2. Управление инцидентами ИБ и обеспечение непрерывности бизнеса

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

Управление непрерывностью бизнеса организации.

Тематика докладов:

1 Информационное право и информационная безопасность.

2 Концепция информационной безопасности.

3 Анализ законодательных актов об охране информационных ресурсов открытого доступа.

4 Анализ законодательных актов о защите информационных ресурсов ограниченного доступа.

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

Примерная тематика практических заданий

Практическая работа 1.

Название работы: Анализ Доктрины информационной безопасности Российской Федерации.

Цель работы: Ознакомиться с нормативным документом, который представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации.

Исходные данные (задание):

1. Прочитайте и проанализируйте Доктрину ИБ РФ.
2. Постройте схему органов государственной власти и самоуправления, отвечающих за информационную безопасность.
3. Определите функциональные обязанности органов государственной власти и самоуправления, отвечающих за информационную безопасность.
4. Определите положения государственной политики в области обеспечения ИБ.
5. Выделите первоочередные мероприятия по обеспечению ИБ, дайте им оценку.

Практическая работа 2.

Название работы: Средства и способы обеспечения информационной безопасности

Цель работы: Текущий контроль полученных знаний и умений.

Исходные данные (задание):

1. Приведите основные методы и приемы защиты обеспечения информационной безопасности в разных информационных пространствах.

Выполнить задание в виде таблице: Виды информационного пространства для организации защиты информации по вариантам

Типовая структура зачетного задания

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

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

Таблица 5

Шкала оценивания		**Формируемые компетенции**	**Индикатор достижения компетенции**	**Критерии оценивания**	**Уровень освоения компетенций**
85 – 100 баллов	**«зачтено»**	**УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач**	**УК-1.1**. 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	
70 – 84 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 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	
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	
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	

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

Факультет экономики, менеджмента и торговли

Кафедра бухгалтерского учета и анализа

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

Б1.О.ДВ.02.02 Основы информационной безопасности

Направление подготовки 38.03.06 Торговое дело

направление (профиль) программы Торговый менеджмент и маркетинг (во внутренней и внешней торговли

Уровень высшего образования *Бакалавриат*

Краснодар – 2021 г.

1.Цель и задачи дисциплины:

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

Задачи дисциплины:

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

2.Содержание дисциплины:

№ п/п	Наименование разделов / тем дисциплины
	Раздел 1. Основные определения и понятия информационной безопасности
1.	Тема 1. Информация как объект защиты. Правовое обеспечение информационной безопасности
2.	Тема 2. Организационное обеспечение информационной безопасности
	Раздел 2. Программно-аппаратные средства и методы обеспечения информационной безопасности
3	Тема 3. Программно-аппаратные средства обеспечения информационной безопасности в информационных сетях.
4.	Тема4. Стандарты и спецификации в области информационной безопасности
Трудоемкость дисциплины составляет 3 з.е. / 108 часа.	

Форма контроля – зачет.

Составитель:
Доцент кафедры бухгалтерского учета и анализа
Краснодарского филиала РЭУ им. Г.В. Плеханова, к.п.н. Салий В.В.