Приложение 3
к основной профессиональной образовательной программе
по направлению подготовки 38.03.01 Экономика
направленность (профиль) программы Финансовая безопасность

Министерство образования и науки 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.В.25 Финансовая кибербезопасность в цифровой экономике

Направление подготовки: 38.03.01 Экономика
Направленность (профиль) программы Финансовая безопасность

Уровень высшего образования ***Бакалавриат***

Год начала подготовки 2023

Краснодар – 2022 г.

Составитель:

к.ю.н., доцент, доцент И.Н. Колкарева

Рабочая программа одобрена на заседании кафедры бухгалтерского учета и анализа Краснодарского филиала РЭУ им. Г.В. Плеханова, протокол № 6 от 10.01 2022 г.

СОДЕРЖАНИЕ

I. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ

Цель и задачи освоения дисциплины

Целью учебной дисциплины **«Финансовая кибербезопасность в цифровой экономике»** является формирование у будущих бакалавров теоретических знаний и практических навыков комплексного анализа понятийного аппарата в сфере финансовой кибербезопасности в информационном обществе, технологий информационной безопасности и умения применять правила кибербезопасности во всех сферах профессиональной деятельности.

Задачи учебной дисциплины **«Финансовая кибербезопасность в цифровой экономике»**:

- формирование у будущих бакалавров представления о том, что представляет собой понятийный аппарат в сфере финансовой кибербезопасности;
- формирование у будущих бакалавров представлений об основах технологий информационной безопасности в цифровой экономике;
- развитие у студентов навыков оценки качества, достаточности и надежности информации по контрагентам, ведение базы данных по клиентам в программном комплексе, составление аналитических заключений, рейтингов, прогнозов с целью предотвращения сделок с недобросовестными партнерами и поддерживания постоянных контактов с данными контрагентами.

Место дисциплины в структуре образовательной программы

Дисциплина «Финансовая кибербезопасность в цифровой экономике» относится к части учебного плана, формируемой участниками образовательных отношений.

Объем дисциплины и виды учебной работы

Таблица 1

Показатели объема дисциплины	**Всего часов по формам обучения**	
	очная	***очно-заочная***
Объем дисциплины в зачетных единицах	***4 ЗЕТ***	
Объем дисциплины в акад.часах	***144***	
Промежуточная аттестация: форма	*Экзамен*	*Экзамен*
Контактная работа обучающихся с преподавателем (Контакт. часы), всего:	**58**	**22**
1. Контактная работа на проведение занятий лекционного и семинарского типов, всего часов, в том числе:	**54**	**18**
• лекции	*24*	*8*
• практические занятия	*30*	*10*
• 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:	**54**	***90***
в том числе:		
• самостоятельная работа в период экз. сессии (СРэк)	32	32
• самостоятельная работа в семестре (СРс)	-	-
в том числе, самостоятельная работа на курсовую работу	-	-
• изучение ЭОР	-	-
• 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)
ПК-1. Мониторинг конъюнктуры рынка банковских услуг, рынка ценных бумаг, иностранной валюты, товарно-сырьевых рынков.	ПК-1.2 Оценка качества, достаточности и надежности информации по контрагентам, ведение базы данных по клиентам в программном комплексе, составление аналитических заключений, рейтингов, прогнозов с целью предотвращения сделок с недобросовестными партнерами.	ПК-1.2. З-1. **Знает** нормативную базу в области финансовой деятельности, основы гражданского, семейного и трудового права, регулирующие финансовые отношения домохозяйств и влияющие на сферу управления личными финансами, основы макроэкономики, микроэкономики, финансовой математики, теории вероятностей и математической статистики. ПК-1.2. У-1. **Умеет** работать в автоматизированных системах информационного обеспечения профессиональной деятельности и производить информационно-аналитическую работу по рынку финансовых продуктов и услуг.
	ПК-1.5 Организация и поддерживание постоянных контактов с рейтинговыми агентствами, аналитиками инвестиционных организаций, консалтинговыми организациями, аудиторскими организациями, оценочными фирмами, государственными и муниципальными органами управления, общественными организациями, средствами массовой информации, информационными, рекламными агентствами.	ПК-1.5. З-1. **Знает** основы социологии, психологии, технологии проведения социологических и маркетинговых исследований ПК-1.5. У-1. **Умеет** работать в автоматизированных системах информационного обеспечения профессиональной деятельности, получать, интерпретировать и документировать результаты исследований, владеть базовыми навыками работы на персональном компьютере.

II. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

этапы формирования и критерии оценивания сформированности компетенций

Для обучающихся очной формы обучения

Таблица 3.

№ 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
		Лекции	Практические занятия	Лабораторные занятия	Практическая подготовка	Самостоятельная Работа/ КЭ, Каттэк,	Всего					
Семестр 8												
Раздел 1. Финансовые технологии в цифровой экономике.												
1.	Тема 1. Особенности информационных взаимодействий в финансовом секторе.	2	2	-	-	5	9	ПК-1.2 ПК-1.5	ПК-1.2. З-1 ПК-1.2. У-1 ПК-1.5. З-1 ПК-1.5. У-1	О.	Т. ПР.	Ин.п.
2.	Тема 2. Современные финансовые технологии. Цифровая трансформация финансовых услуг.	2	2	-	-	5	9	ПК-1.2 ПК-1.5	ПК-1.2. З-1 ПК-1.2. У-1 ПК-1.5. З-1 ПК-1.5. У-1	О.	З.	Ин.п.
3.	Тема 3. Влияние цифровых технологий на развитие банковской сферы.	2	4			5	11	ПК-1.2 ПК-1.5	ПК-1.2. З-1 ПК-1.2. У-1	О.	ПР	Ин.п.
4.	Тема 4. Цифровизация страхового рынка.	2	4			5	11	ПК-1.2 ПК-1.5	ПК-1.2. З-1 ПК-1.2. У-1	О.	ПР	Ин.п.

Раздел 2. Финансовая кибербезопасность: общие положения.												
5.	Тема 5. Концепция (стратегия) национальной информационной безопасности Российской Федерации. Законодательство в сфере финансовой кибербезопасности.	2	2	-	-	6	10	ПК-1.2 ПК-1.5	ПК-1.2. З-1 ПК-1.2. У-1	О.	З.	Ин.п.
6.	Тема 6. Современные угрозы в цифровом секторе.	2	4			6	12	ПК-1.2 ПК-1.5	ПК-1.2. З-1 ПК-1.2. У-1 ПК-1.5. З-1 ПК-1.5. У-1	О.	К.	Ин.п.
7.	Тема 7. Финансовая кибербезопасность в РФ: угрозы и противодействие им.	2	2	-	-	6	10	ПК-1.2 ПК-1.5	ПК-1.2. З-1 ПК-1.2. У-1 ПК-1.5. З-1 ПК-1.5. У-1	О.	ПР.	Ин.п.
Раздел 3. Киберпреступность и способы её предотвращения в финансовой сфере.												
8.	Тема 8. Преступления в сфере информационных технологий.	2	4			6	12	ПК-1.2 ПК-1.5	ПК-1.2. З-1 ПК-1.2. У-1	О.	ПР.	Ин.п.
9	Тема 9. Хакеры и проблемы обеспечения финансовой безопасности.	4	2			6	12	ПК-1.2 ПК-1.5	ПК-1.2. З-1 ПК-1.2. У-1	О.	ПР	Ин.п.
10.	Тема 10. Международное сотрудничество в сфере финансовой кибербезопасности.	4	4			4	12	ПК-1.2 ПК-1.5	ПК-1.2. З-1 ПК-1.2. У-1 ПК-1.5. З-1 ПК-1.5. У-1	О.	ПР.	Ин.п.
	Консультация перед экзаменом (КЭ)	-	-	-	-	-/2	2					
	Контактная работа по промежуточной аттестации (Катт)	-	-	-	-	-/2	2					
	Самостоятельная работа в период экз. сессии (СРэк)	-	-	-	-	32/-	32					

	Итого	**24**	**30**	**-**	**-**	**86/4**	**144**					

этапы формирования и критерии оценивания сформированности компетенций

Для обучающихся очно-заочной 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 8												
Раздел 1. Финансовые технологии в цифровой экономике.												
1.	Тема 1. Особенности информационных взаимодействий в финансовом секторе.	0,5	1	-	-	8	9,5	ПК-1.2 ПК-1.5	ПК-1.2. З-1 ПК-1.2. У-1 ПК-1.5. З-1 ПК-1.5. У-1	О.	Т. ПР.	Ин.п.
2.	Тема 2. Современные финансовые технологии. Цифровая трансформация финансовых услуг.	0,5	1	-	-	10	11,5	ПК-1.2 ПК-1.5	ПК-1.2. З-1 ПК-1.2. У-1 ПК-1.5. З-1 ПК-1.5. У-1	О.	З.	Ин.п.
3.	Тема 3. Влияние цифровых технологий на развитие банковской сферы.	0,5	1			10	11,5	ПК-1.2 ПК-1.5	ПК-1.2. З-1 ПК-1.2. У-1	О.	ПР	Ин.п.
4.	Тема 4. Цифровизация страхового рынка.	0,5	1			8	9,5	ПК-1.2 ПК-1.5	ПК-1.2. З-1 ПК-1.2. У-1	О.	ПР	Ин.п.
Раздел 2. Финансовая кибербезопасность: общие положения.												

5.	Тема 5. Концепция (стратегия) национальной информационной безопасности РФ.	1	1	-	-	10	12	ПК-1.2 ПК-1.5	ПК-1.2. З-1 ПК-1.2. У-1	О.	З.	Ин.п.
6.	Тема 6. Современные угрозы в цифровом секторе.	1	1			10	12	ПК-1.2 ПК-1.5	ПК-1.2. З-1 ПК-1.2. У-1 ПК-1.5. З-1 ПК-1.5. У-1	О.	К.	Ин.п.
7.	Тема 7. Финансовая кибербезопасность в РФ: угрозы и противодействие им.	1	1	-	-	10	12	ПК-1.2 ПК-1.5	ПК-1.2. З-1 ПК-1.2. У-1 ПК-1.5. З-1 ПК-1.5. У-1	О.	ПР.	Ин.п.
Раздел 3. Киберпреступность и способы её предотвращения в финансовой сфере.												
8.	Тема 8. Преступления в сфере информационных технологий.	1	1			8	10	ПК-1.2 ПК-1.5	ПК-1.2. З-1 ПК-1.2. У-1	О.	ПР.	Ин.п.
9	Тема 9. Хакеры и проблемы обеспечения финансовой безопасности.	1	1			8	10	ПК-1.2 ПК-1.5	ПК-1.2. З-1 ПК-1.2. У-1	О.	ПР	Ин.п.
10.	Тема 10. Международное сотрудничество в сфере финансовой кибербезопасности.	1	1			8	10	ПК-1.2 ПК-1.5	ПК-1.2. З-1 ПК-1.2. У-1 ПК-1.5. З-1 ПК-1.5. У-1	О.	ПР.	Ин.п.
	Консультация перед экзаменом (КЭ)	-	-	-	-	-/2	2					
	Контактная работа по промежуточной аттестации (Катт)	-	-	-	-	-/2	2					
	Самостоятельная работа в период экз. сессии (СРэк)	-	-	-	-	32/-	32					
	Итого	**8**	**10**	**-**	**-**	**122/4**	**144**					

Формы учебных заданий на аудиторных занятиях:

Опрос (О.)

Формы текущего контроля:

Тест (Т.)

Кейс (К.)

Подготовка презентаций (ПР.) Задачи (З.)

Формы заданий для творческого рейтинга:

Индивидуальный проект (Ин.п.)

III. УЧЕБНО-МЕТОДИЧЕСКОЕ И МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Рекомендуемая литература

Основная литература:

1. Авдийский, В. И. Теневая экономика и экономическая безопасность государства: учебное пособие / В.И. Авдийский, В.А. Дадалко, Н.Г. Синявский. - 3-е изд., перераб. и доп. - Москва: ИНФРАМ, 2021. - 538 с. - (Высшее образование: Бакалавриат). - DOI 10.12737/24758. - ISBN 978-5-16- 012671-5 URL: https://znanium.com/catalog/product/1234924

2. Губернаторова, Н.Н., Финансовая безопасность: учебное пособие / Н.Н. Губернаторова. — Москва: КноРус, 2021. — 181 с. — ISBN 978-5-406-07986-7. — URL:https://book.ru/book/938855.

3. Козьминых, С.И., Информационная безопасность финансово-кредитных организаций в условиях цифровой трансформации экономики : монография / С.И. Козьминых. — Москва: КноРус, 2021. — 281 с. — ISBN 978-5-406-08948-4. — URL:https://book.ru/book/941548.

4. Овчинский, В. С. Основы борьбы с киберпреступностью и кибертерроризмом: хрестоматия / сост. В. С. Овчинский. — Москва: Норма: ИНФРА-М, 2022. — 528 с. - ISBN 978-5-91768-814-5. - Текст : электронный. - URL: https://znanium.com/read?id=387641

5. Финансовая безопасность и право в эпоху цифровизации : сборник статей / С.В. Запольский, Е.Л. Васянина, С.О. Шохин [и др.] ; под общ. ред. М. Н. Кобзарь-Фроловой. — Москва: Русайнс, 2022. — 121 с. — ISBN 978-5-4365-8160-6. — URL:https://book.ru/book/943433.

Дополнительная литература:

1. Бриллиантов, А. В. Преступления в сфере экономической деятельности [Электронный ресурс]: учебное пособие / А. В. Бриллиантов, Е. Ю. Четвертакова. - Электрон. текстовые данные. - М.: Российский государственный университет правосудия, 2019. -108 с.- 978-5-93916-657-7. - Режим доступа: http://www.iprbookshop.ru/78309.html.

2. Беликов, Е.Г., Безопасность в бюджетно-налоговой, таможенной и иных сферах финансовой деятельности: экономические и правовые проблемы: сборник статей / Е.Г. Беликов. — Москва: Русайнс, 2022. — 374 с. — ISBN 978-5-4365-9289-3. — URL:https://book.ru/book/944179

3. Козьминых, С.И., Информационная безопасность в банковско-финансовой сфере. Сборник научных работ участников ежегодной международной молодежной научно-практической конференции в рамках VI (Международного форума «Как попасть в пятерку?» 28 ноября 2019 года : сборник статей / С.И. Козьминых. — Москва : Русайнс, 2022. — 205 с. — ISBN 978-5-4365-0617-3. — URL:https://book.ru/book/943691

4. Экономическая безопасность : учебник / под общ. ред. С.А. Коноваленко. - Москва : ИНФРА-М, 2021. - 526 с. - (Высшее образование: Специалитет). - DOI 10.12737/1048684. - ISBN 978-5-16- 015729-0 URL: https://znanium.com/catalog/product/1048684

5.Основы цифровой грамотности и кибербезопасности: учеб. пособие/Т. А. Бороненко, А. В. Кайсина, И. Н. Пальчикова, Е. В. Федоркевич, В. С. Федотова. – СПб.: ЛГУ им. А.С. Пушкина, 2021 https://www.elibrary.ru/item.asp?id=46991584

Нормативные правовые документы:

1. Конституция Российской Федерации (принята на референдуме 12 декабря 1993 года) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12. 2008 № 6-ФКЗ, от 30.12. 2008 № 7-ФКЗ, от 05.02. 2014. № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ) // РГ. 1994. 25 января; СЗ РФ. 2014. № 30. Ст. 4202. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_28399/

2. Гражданский кодекс Российской Федерации (часть первая) от 03.11.1994 № 51-ФЗ // СЗ РФ. 1994. № 32. Ст. 3301; СЗ РФ. 2019. № 29 (часть 1). Ст. 3844. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_5142/

3. Гражданский процессуальный кодекс Российской Федерации от 14. 11. 2002 № 138-ФЗ // Консультант Плюс [Электронный ресурс]: справочная правовая система. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_39570/

4. Кодекс Российской Федерации об административных правонарушениях» от 30.12.2001 № 195-ФЗ // СЗ РФ. 2016. № 27 (часть 1). Ст. 4089. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_34661/

5. Налоговый кодекс Российской Федерации (часть вторая) от 05.08.2000 № 117-ФЗ // СЗ РФ. 2000. № 32. Ст. 3340; СЗ РФ. 2019. № 31. Ст. 4427. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_28165/

6.Уголовный кодекс РФ от 13.06.1996 г. № 63 ФЗ// Консультант Плюс [Электронный ресурс]: справочная правовая система. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_10699/

7. Федеральный закон от 10.07.2002 № 86-ФЗ «О Центральном Банке Российской Федерации (Банке России)» // РГ. 2002. 13 июля; СЗ РФ. 2019. № 31. Ст. 4430. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_37570/

8. Федеральный закон от 28.06.2013 № 134-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части противодействия незаконным финансовым операциям» // СЗ РФ. 2013. № 26. Ст. 3207. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_148268/

9. Федеральный закон от 26.07.2006 № 135-ФЗ «О защите конкуренции» // СЗ РФ. 2006. № 31 (часть 1). Ст. 3434; 2019. № 29 (часть I). Ст. 3854. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_149702/.

Федеральный закон от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» // СЗ РФ. 2001. № 33 (часть 1). Ст. 3418; СЗ РФ. 2019. № 31. Ст. 4430. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_32834/

10. Федеральный закон от 27.06.2011 № 161-ФЗ «О национальной платежной системе» // СЗ РФ. 2011. № 27. Ст. 3872; СЗ РФ. 2019. Ст. 4423. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_115625/

11. Федеральный закон Российской Федерации «О противодействии коррупции» // Российская газета. 2008. 30 декабря. № 4823; СЗ РФ. 2019. № 30. Ст.4153. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_82959/

12. 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/

13. Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы" [Электрон.ресурс]. – Режим доступа http://www.consultant.ru/document/cons_doc_LAW_216363

14. Федеральный закон от 12 августа 1995 г. N 144-ФЗ «Об оперативно-розыскной деятельности». // СЗ РФ. 1995. № 33. Ст. 3349. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_7519/

15. Федеральный закон от 31 мая 2001 г. № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации». // СЗ РФ. 2001. № 23. Ст. 2291 Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_31871/

ПЕРЕЧЕНЬ ИНФОРМАЦИОННО-СПРАВОЧНЫХ СИСТЕМ

1. http://www.consultant.ru - Справочно-правовая система Консультант Плюс;

ПЕРЕЧЕНЬ ЭЛЕКТРОННО-ОБРАЗОВАТЕЛЬНЫХ РЕСУРСОВ

отсутствуют

ПЕРЕЧЕНЬ ПРОФЕССИОНАЛЬНЫХ БАЗ ДАННЫХ

1. http://www.gks.ru - Росстат – федеральная служба государственной статистики
2. https://www.nalog.ru/rn39/program/- База программных средств налогового учета
3. https://www.polpred.com - Электронная база данных «Polpred.com Обзор СМИ»
4. http://www.rags.ru/gosts/2874/ - Российский архив государственных стандартов, а также строительных норм и правил (СНиП) и образцов юридических документов (РАГС)
5. http://www.isras.ru/Databank.html -Архивный банк данных Института социологии Российской академии наук.

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

1. http://www.duma.gov.ru/ - Сайт Государственной Думы Российской Федерации.
2. http://www.ksrf.ru Официальный сайт Конституционного Суда Российский Федерации.
3. http://www.vsrf.ru/ Сайт Верховного Суда Российской Федерации.
4. https://www.cbr.ru/ Официальный сайт Банка России (статистические данные по финансовому рынку).
5. http://www.gks.ru/ Официальный сайт Федеральной службы государственной статистики РФ (статистические данные).
6. https://www.minfin.ru/ru/?fullversion=1- Официальный сайт Министерства финансов РФ.
7. http://roskazna.ru/ Официальный сайт Казначейства России.
8. https://www.nalog.ru/ Официальный сайт Федеральной налоговой службы.
9. http://pravo.gov.ru/ Официальный интернет портал правовой информации.
10. http://www.fssprus.ru Официальный сайт Федеральной службы судебных приставов.
11. http://www.lawportal.ru/ «Юридическая Россия» – российский образовательный правовой портал.
12. http://www.pravopoliten.ru/ – Энциклопедия российского права.
13. http://sudrf.ru/ – Государственная автоматизированная система РФ «Правосудие».

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)
АнтивирусDr.Web Desktop Security Suite Комплексная защита
Браузер Google Chrome
Adobe Premiere

МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Дисциплина «Финансовая кибербезопасность в цифровой экономике» обеспечена:

а) для проведения занятий лекционного типа:

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

б) для проведения занятий семинарского типа (практические занятия):

– учебной аудиторией, оборудованной учебной мебелью и техническими средствами обучения, служащими для представления учебной информации;

в) для самостоятельной работы:

– 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 подготовке и оформлению рефератов.

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 «Финансовая кибербезопасность в цифровой экономике» 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 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 «*Финансовая кибербезопасность в цифровой экономике*» учебным планом не предусмотрена*

Перечень вопросов к экзамену:

Номер вопроса	Перечень вопросов к экзамену
1.	Мировые тенденции развития технологий big data.
2.	Перспективы использования нейротехнологий и технологий искусственного интеллекта в информационных системах и технологиях управления финансами.
3.	Мировые тенденции развития технологии блокчейн.
4.	Промышленный интернет: направления развития.
5.	Перспективы использования технологий виртуальной и дополненной реальности в информационных системах цифровой экономики.
6.	Нормативное регулирование цифровой экономики.
7.	Мероприятия Правительства РФ по направлению "Информационная безопасность" программы "Цифровая экономика Российской Федерации".
8.	Стандарты информационной безопасности технологий цифровой экономики.
9.	Национальные стандарты безопасности киберфизических систем.
10.	Требования к киберфизическим системам на объектах критической инфраструктуры.
11.	Национальные рамки кибербезопасности.
12.	Информационная безопасность как необходимое условие развития экономики цифрового типа.
13.	Показатели уровня информационной безопасности сквозных технологий цифровой экономики.
14.	Общие проблемы обеспечения безопасности информационной технологии цифровой экономики.
15.	Защита информации при использовании технологии big data в информационных системах и технологиях управления бизнес-процессами.

Номер вопроса	Перечень вопросов к экзамену
16.	Защита информации при применении нейротехнологий и технологий искусственного интеллекта в информационных системах и технологиях управления бизнес-процессами.
17.	Нормативно-правовые акты и стандарты по кибербезопасности.
18.	Понятие информации и информатизации, свойства информации как объекта защиты от киберугроз.
19.	Финансовая кибербезопасность в РФ: угрозы и противодействие им.
20.	Цифровизация страхового рынка.
21.	Влияние цифровых технологий на развитие банковской сферы.
22.	Современные финансовые технологии. Цифровая трансформация финансовых услуг.
23.	Особенности информационных взаимодействий в финансовом секторе.
24.	Современные угрозы в цифровом секторе.
25.	Преступления в сфере информационных технологий.
26.	Хакеры и проблемы обеспечения финансовой безопасности.
27.	Международное сотрудничество в сфере финансовой кибербезопасности.
28.	Международные организации по кибербезопасности.
29.	Формирование требований к построению систем криптографической и стеганографической защиты.
30.	Сетевая безопасность и управление процессом обеспечения безопасности.
31.	Неправомерный доступ к компьютерной информации.
32.	Создание, использование и распространение вредоносных компьютерных программ.
33.	Система внутреннего контроля как элемент системы противодействия киберпреступности.
34.	Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.
35.	Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации.
36.	Особенности и проблемы противодействия цифровой преступности.
37.	Понятие и особенности цифровой преступности.

Номер вопроса	Перечень вопросов к экзамену
38.	Риск разглашения конфиденциальной информации.
39.	Мониторинг, прогнозирование и планирование предупреждения цифровой преступности.
40.	Предупреждение преступлений, совершаемых в условиях цифровой трансформации.

Перечень практических заданий к экзамену

Номер задания	Перечень практических заданий к экзамену
1.	**Задание 1.** Разработайте сценарий нападения со стороны сервера, например, использование слабых конфигураций, имитация ИП (IP), обеспечение отказа / дистрибутивного отказа в обслуживании (DoS и DDoS), внедрение SQL и переполнение сетевого буфера на основе протоколов.
2.	**Задача 2.** В ходе работы сервера сборщика и анализатора качества кода было выявлено подозрительное поведение. В исходных кодах хранимого программного обеспечения появлялись артефакты, которые были внесены в автоматическом режиме. Сетевое взаимодействие сервера с внешними ресурсами возросло, а сами сервисы стали работать со сбоями и ошибками. Поскольку сервис непрерывно дорабатывается под нужды технических отделов компании высока вероятность появления уязвимостей, которые возможно были поэксплуатированы злоумышленниками. Системные администраторы заверили, что сервера в ЦОДе работают стабильно и в ремонте не нуждаются, очевидно, сбои происходят из-за ошибок в программном коде сервиса и/или логике его работы. Вам будут предоставлены адреса, дампы памяти, операционных систем, образы и исполняемые файлы для анализа. Необходимо провести анализ.
3.	**Задача 3.** В случае получения доступа к процессингу платежных карт привлекаются соучастники, занимающиеся оформлением на подставных лиц платежных карт атакованной организации. Данные карты консолидируются в руках лиц, занимающихся получением денежных средств. Их задача - обеспечить снятие денежных средств в банкоматах непосредственно после того, как балансы и лимиты карт будут повышены в системе процессинга. В процессе получения денег соучастниками оператор может при необходимости продолжать поднимать лимиты по снятию или балансы карт. Каким образом им противостоять? Кто будет нести ответственность за утрату денежных средств?
4.	**Задание 4.** Чем обусловлена объективность угроз финансовой безопасности хозяйствующего субъекта?
5.	**Задание 5.** В соответствии с объектом финансовой безопасности выделяются виды финансовых угроз: а) реализованные; б) угрозы упущенных выгод; в) умышленные; г) все ответы верны.

6.	**Задание 6.** Описать укрепление безопасности на сетевом периметре и усовершенствование безопасности на сервере.
7.	**Задание 7. Выберите утверждение, которое вы считаете наиболее точным.** Все сотрудники должны пройти обучение по обнаружению признаков кибератаки. Конкретные сотрудники (например, ИТ-специалисты) должны пройти обучение по обнаружению признаков кибератаки. Если на предприятии установлено хорошее антивирусное программное обеспечение, персоналу не нужно проходить обучение по обнаружению признаков кибератаки.
8.	**Задание 8.** Во всплывающем окне на рабочем столе сообщается, что для загруженного надежного приложения по проверке правописания доступно новое обновление. Как поступить в данной ситуации правильно?
9.	**Задание 9.** Определите тип и основные характеристики личности цифрового экономического преступника.
10.	**Задание 10.** Определите детерминанты экономической цифровой преступности.
11.	**Задача 11.** Определите основные меры противодействия экономической цифровой преступности.
12.	**Задание 12.** Вы решили проверить баланс своей карты через интернет. Зашли на страницу сайта банка, но на первый взгляд показалось, что сайт выглядит необычно: расплывчатый логотип, в строке браузера указано не название банка, а какое-то другое слово, не все ссылки открываются. Что Вы будете делать?
13.	**Задание 13.** Определите причины и условия, способствующие преступной деятельности с использованием финансовых инструментов в цифровой среде.
14.	**Задача 14.**. Организованные преступные группы начинают компрометировать платежи, связанные с использованием бесконтактных карт (NFC). Какие меры безопасности могут помогать в эффективной борьбе с карточным мошенничеством?
15.	**Задание 15.** Назовите международные организации, формирующие общие положения о противодействии преступной деятельности с использованием финансовых инструментов в цифровой среде.
16.	**Задание 16.** Определите роль государственной политики в сфере обеспечения цифровой безопасности.
17.	**Задание 17.** Какое влияние оказывает законодательное регулирование на динамику преступлений, совершаемых с использованием виртуальных валют (криптовалют)?
18.	**Задание 18.** Звонок из Министерства труда и социальной защиты. Вам рассказывают про пособие, которое положено выпускнику организации для детей-сирот. Чтобы перевестиденьги на карту, необходимо сообщить ее данные звонящему. Ваши действия?
19.	**Задача 19.** Назовите документы, регулирующие государственную политику в сфере обеспечения цифровой безопасности.
20.	**Задача 20.** Компания Yahoo Inc. (теперь известная под названием Altaba) сообщила об одном случае (из нескольких случаев) утечки данных, с которым

	она столкнулась, спустя два года после инцидента. В результате такого раскрытия информации «цена акций Yahoo упала на 3 процента, что привело к потере около 1,3 миллиардов долларов США рыночной капитализации. Кроме того, компания, которая [в тот момент времени] вела переговоры о продаже своего бизнеса компании Verizon, была вынуждена согласиться со скидкой в размере 7,25 процентов на предложенную цену покупки, что снизило ее на 350 млн. долларов США». Из-за несвоевременного раскрытия сведений об утечке данных какие санкции должны быть наложены на компанию?
21.	**Задание 21.** Определите, является ли Президент РФ субъектом контроля в сфере кибербезопасности и какие полномочия он осуществляет?
22.	**Задание 22.** На примере данных на электронных носителях проведите 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.
23.	**Задание 23.** На примере телефонной базы ограниченного пользования проведите 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.
24.	**Задание 24.** Назовите количественные и качественные характеристики экономической цифровой преступности.
25.	**Задание 25.** Дайте оценку рисков использования виртуальных валют (криптовалют) представителями организованных преступных формирований.
26.	**Задание 26**. «Преступление-в-качестве-услуги» и «подпольные цифровыеуслуги» Она объединяет между собой специализированных поставщиков хакерских утилит и организованные преступные группировки. В чём их смысл и способы совершения?
27.	**Задача 27.** Киберпреступники могут также использовать анонимные сети для шифрования (т.е. блокирования доступа) трафика и скрытия адреса Интернет-протокола (или IP-адреса), «уникального идентификатора, присваиваемого компьютеру [или другому подключенному к Интернету цифровому устройству] поставщиком услуг Интернета при подключении к сети», чтобы скрыть свою активность в Интернете и свое местонахождение. Какие хорошо изученные примеры анонимных сетей пользуются злоумышленники?
28.	**Задание 28.** Назовите основные направления государственной политики в сфере обеспечения цифровой безопасности.
29.	**Задача 29.** На примере почтового сервера проведите 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.
30.	**Задание 30. Перечислите у**грозы информационной кибербезопасности в сетях финансовых организации.
31.	**Задание 31.** Назовите основные способы внедрения информационных систем для упрощения возврата денег жертвам киберпреступников.
32.	**Задание 32.** Опишите примеры противодействия несанкционированным финансовым операциям.

Типовые тестовые задания:

1. К правовым методам, обеспечивающим информационную безопасность, относятся:

а) разработка аппаратных средств обеспечения правовых данных;
б) разработка и установка во всех компьютерных правовых сетях журналов учета действий;
в) разработка и конкретизация правовых нормативных актов обеспечения безопасности.

2. Основными источниками угроз финансовой кибербезопасности являются:

а) хищение жестких дисков, подключение к сети, инсайдерство
б) перехват данных, хищение данных, изменение архитектуры системы
в) хищение данных, подкуп системных администраторов, нарушение регламента работы

3. Виды информационной безопасности:

а) персональная, корпоративная, государственная
б) клиентская, серверная, сетевая
в) локальная, глобальная, смешанная

4. Цели финансовой кибербезопасности – своевременное обнаружение, предупреждение:

а) несанкционированного доступа, воздействия в сети
б) инсайдерства в организации
в) чрезвычайных ситуаций

5. Основные объекты информационной безопасности:

а) компьютерные сети, базы данных
б) информационные системы, психологическое состояние пользователей
в) бизнес-ориентированные, коммерческие системы

6. Основными рисками информационной безопасности являются:

а) искажение, уменьшение объема, перекодировка информации
б) техническое вмешательство, выведение из строя оборудования сети
в) потеря, искажение, утечка информации

7. К основным принципам обеспечения финансовой кибербезопасности относится:

а) экономической эффективности системы безопасности
б) многоплатформенной реализации системы
в) усиления защищенности всех звеньев системы

8. Основными субъектами информационной безопасности являются:

а) руководители, менеджеры, администраторы компаний
б) органы права, государства, бизнеса

в) сетевые базы данных, фаерволлы

9. К основным функциям системы безопасности можно отнести:

а) установление регламента, аудит системы, выявление рисков
б) установка новых офисных приложений, смена хостинг-компании
в) внедрение аутентификации, проверки контактных данных пользователей

10. Принципом финансовой кибербезопасности является принцип недопущения:

а) неоправданных ограничений при работе в сети (системе)
б) рисков безопасности сети, системы
в) презумпции секретности.

Примеры вопросов для опроса:

1. Каковы основные положения программы "Цифровая экономика Российской Федерации"?
2. Какой документ правительства регламентирует вопросы информационной безопасности программы "Цифровая экономика Российской Федерации"?
3. Какие стандарты обеспечения информационной безопасности имеют отношение к цифровой экономике?
4. Назначение, область применения и направления развития стандарта ГОСТ Р 53110-2008. ОСТ Р 53110-2008. Система обеспечения информационной безопасности сети связи общего пользования.
5. Какие направления деятельности технического комитета «Киберфизические системы» вы знаете?
6. Какие показатели характеризуют уровень информационной безопасности сквозных технологий цифровой экономики в заданной предметной области?
7. Каковы результаты анализа уровня защиты заданной информационной технологии цифровой экономики в заданной предметной области?
8. Какие направления развития средств защиты информационных технологий цифровой экономики в заданной предметной области вы считаете перспективными?
9. Выработайте рекомендации по внедрению и развитию средств защиты информационных технологий цифровой экономики в заданной предметной области.

Типовые кейсы:

Кейс (проблемная ситуация):

Задача 1. Во время карантина несколько тысяч сотрудников АКБ «Нева» переходили на удаленную работу. Нужно было увеличить скорость портов, чтобы сотрудники могли подключаться ко внутренним сервисам банка из дома. Эти порты важно было защитить, чтобы злоумышленники не могли остановить работу банка с помощью DDoS-атаки. Какие формы защиты от злоумышленников следует предусмотреть на предприятии?

Задача 2. Веб-сайт электронного банка E-Bank был отключен от сети, что препятствует доступу клиентов к веб-сайту. Вас наняли для проведения расследования киберпреступления. У вас есть подозрение, что имела место DDoS-атака. С какими препятствиями вы бы могли столкнуться при проведении своего расследования? Какие шаги вы предпримете, чтобы попытаться установить личность исполнителя или исполнителей этого киберпреступления?

Задание: Выберите утверждение, которое вы считаете наиболее точным.

Все сотрудники должны пройти обучение по обнаружению признаков кибератаки.

Конкретные сотрудники (например, ИТ-специалисты) должны пройти обучение по обнаружению признаков кибератаки.

Если на предприятии установлено хорошее антивирусное программное обеспечение, персоналу не нужно проходить обучение по обнаружению признаков кибератаки.

Студентам предлагается проанализировать законность указанных требований и разрешить ситуацию с точки зрения действующего законодательства.

Примерная тематика рефератов (презентаций, докладов) к теме 5. **Концепция (стратегия) национальной информационной безопасности Российской Федерации. Законодательство в сфере финансовой кибербезопасности.**

1. Технология предотвращения основных угроз финансовой кибербезопасности.
2. Система обеспечения национальной безопасности: понятие, сущность и структура.
3. Основные цели, задачи и принципы обеспечения финансовой кибербезопасности.
4. Национальные интересы России в сфере финансовой кибербезопасности: понятие и их особенности.
5. Политика финансовой кибербезопасности: цели, задачи и основные направления.
6. Методы анализа системы обеспечения национальной финансовой кибербезопасности.
7. Место и роль органов государственной власти в разработке современной Концепции национальной безопасности Российской Федерации.
8. Технология управления процессом обеспечения национальной финансовой кибербезопасности.
9. Роль органов государственной власти в создании эффективной системы обеспечения национальной безопасности.

Типовая структура экзаменационного задания

Наименование оценочного средства	***Максимальное количество баллов***
Вопрос 1. Нормативное регулирование цифровой экономики.	*15*
Вопрос 2. Международные организации по кибербезопасности.	*15*
Практическое задание. Опишите 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

Шкала оценивания		Формируемые компетенции	Индикатор достижения компетенции	Критерии оценивания	Уровень освоения компетенций
85 – 100 баллов	**«отлично»**	ПК-1. Мониторинг конъюнктуры рынка банковских услуг, рынка ценных бумаг, иностранной валюты, товарно-сырьевых рынков.	ПК-1.2 Оценка качества, достаточности и надежности информации по контрагентам, ведение базы данных по клиентам в программном комплексе, составление аналитических заключений, рейтингов, прогнозов с целью предотвращения сделок с недобросовестными партнерами.	**Знает верно и в полном объеме:** нормативную базу в области финансовой деятельности, основы гражданского, семейного и трудового права, регулирующие финансовые отношения домохозяйств и влияющие на сферу управления личными финансами, основы макроэкономики, микроэкономики, финансовой математики, теории вероятностей и математической статистики. **Умеет верно и в полном объеме:** работать в автоматизированных системах информационного обеспечения профессиональной деятельности и производить информационно-аналитическую работу по рынку финансовых продуктов и услуг.	**Продвинутый**
			ПК-1.5 Организация и поддерживание постоянных контактов с рейтинговыми агентствами, аналитиками инвестиционных организаций, консалтинговыми организациями, аудиторскими организациями, оценочными фирмами, государственными и муниципальными	**Знает верно и в полном объеме:** основы социологии, психологии, технологии проведения социологических и маркетинговых исследований **Умеет верно и в полном объеме:** работать в автоматизированных системах информационного обеспечения профессиональной деятельности, получать, интерпретировать и документировать результаты	

			органами управления, общественными организациями, средствами массовой информации, информационными, рекламными агентствами.	исследований, владеть базовыми навыками работы на персональном компьютере.	
70 – 84 баллов	**«хорошо»**	ПК-1. Мониторинг конъюнктуры рынка банковских услуг, рынка ценных бумаг, иностранной валюты, товарно-сырьевых рынков.	ПК-1.2 Оценка качества, достаточности и надежности информации по контрагентам, ведение базы данных по клиентам в программном комплексе, составление аналитических заключений, рейтингов, прогнозов с целью предотвращения сделок с недобросовестными партнерами.	**Знает с незначительными замечаниями:** нормативную базу в области финансовой деятельности, основы гражданского, семейного и трудового права, регулирующие финансовые отношения домохозяйств и влияющие на сферу управления личными финансами, основы макроэкономики, микроэкономики, финансовой математики, теории вероятностей и математической статистики. **Умеет с незначительными замечаниями:** работать в автоматизированных системах информационного обеспечения профессиональной деятельности и производить информационно-аналитическую работу по рынку финансовых продуктов и услуг.	**Повышенный**
			ПК-1.5 Организация и поддерживание постоянных контактов с рейтинговыми агентствами, аналитиками инвестиционных организаций, консалтинговыми	**Знает с незначительными замечаниями:** основы социологии, психологии, технологии проведения социологических и маркетинговых исследований **Умеет с незначительными замечаниями:** работать	

			организациями, аудиторскими организациями, оценочными фирмами, государственными и муниципальными органами управления, общественными организациями, средствами массовой информации, информационными, рекламными агентствами.	в автоматизированных системах информационного обеспечения профессиональной деятельности, получать, интерпретировать и документировать результаты исследований, владеть базовыми навыками работы на персональном компьютере.	
50 – 69 баллов	**«удовлетворительно»**	ПК-1. Мониторинг конъюнктуры рынка банковских услуг, рынка ценных бумаг, иностранной валюты, товарно-сырьевых рынков.	ПК-1.2 Оценка качества, достаточности и надежности информации по контрагентам, ведение базы данных по клиентам в программном комплексе, составление аналитических заключений, рейтингов, прогнозов с целью предотвращения сделок с недобросовестными партнерами.	**Знает на базовом уровне:** нормативную базу в области финансовой деятельности, основы гражданского, семейного и трудового права, регулирующие финансовые отношения домохозяйств и влияющие на сферу управления личными финансами, основы макроэкономики, микроэкономики, финансовой математики, теории вероятностей и математической статистики. **Умеет на базовом уровне:** работать в автоматизированных системах информационного обеспечения профессиональной деятельности и производить информационно-аналитическую работу по рынку финансовых продуктов и услуг.	**Базовый**
			ПК-1.5 Организация и поддерживание постоянных контактов с рейтинговыми	**Знает на базовом уровне:** основы социологии, психологии, технологии проведения социологических и	

			агентствами, аналитиками инвестиционных организаций, консалтинговыми организациями, аудиторскими организациями, оценочными фирмами, государственными и муниципальными органами управления, общественными организациями, средствами массовой информации, информационными, рекламными агентствами.	маркетинговых исследований **Умеет на базовом уровне:** работать в автоматизированных системах информационного обеспечения профессиональной деятельности, получать, интерпретировать и документировать результаты исследований, владеть базовыми навыками работы на персональном компьютере.	
менее 50 баллов	**«неудовлетворительно»**	ПК-1. Мониторинг конъюнктуры рынка банковских услуг, рынка ценных бумаг, иностранной валюты, товарно-сырьевых рынков.	ПК-1.2 Оценка качества, достаточности и надежности информации по контрагентам, ведение базы данных по клиентам в программном комплексе, составление аналитических заключений, рейтингов, прогнозов с целью предотвращения сделок с недобросовестными партнерами.	**Не знает на базовом уровне:** нормативную базу в области финансовой деятельности, основы гражданского, семейного и трудового права, регулирующие финансовые отношения домохозяйств и влияющие на сферу управления личными финансами, основы макроэкономики, микроэкономики, финансовой математики, теории вероятностей и математической статистики. **Не умеет на базовом уровне:** работать в автоматизированных системах информационного обеспечения профессиональной деятельности и производить информационно-аналитическую работу по рынку финансовых продуктов и услуг.	**Компетенции не сформированы**
			ПК-1.5	**Не знает на базовом**	

			Организация и поддерживание постоянных контактов с рейтинговыми агентствами, аналитиками инвестиционных организаций, консалтинговыми организациями, аудиторскими организациями, оценочными фирмами, государственными и и муниципальными органами управления, общественными организациями, средствами массовой информации, информационными, рекламными агентствами.	**уровне:** основы социологии, психологии, технологии проведения социологических и маркетинговых исследований **Не умеет на базовом уровне:** работать в автоматизированных системах информационного обеспечения профессиональной деятельности, получать, интерпретировать и документировать результаты исследований, владеть базовыми навыками работы на персональном компьютере.	

Приложение

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

Кафедра бухгалтерского учета и анализа

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

Б1.В.25 ФИНАНСОВАЯ КИБЕРБЕЗОПАСНОСТЬ В ЦИФРОВОЙ ЭКОНОМИКЕ

Направление подготовки: 38.03.01 Экономика
Направленность (профиль) программы Финансовая безопасность

Уровень высшего образования ***Бакалавриат***

Краснодар
2022 г.

1. Цель и задачи дисциплины.

Целью учебной дисциплины «***Финансовая кибербезопасность в цифровой экономике***» является формирование у будущих бакалавров теоретических знаний и практических навыков комплексного анализа понятийного аппарата в сфере финансовой кибербезопасности в информационном обществе, технологий информационной безопасности и умения применять правила кибербезопасности во всех сферах профессиональной деятельности.

Задачи учебной дисциплины «***Финансовая кибербезопасность в цифровой экономике***»:

- формирование у будущих бакалавров представления о том, что представляет собой понятийный аппарат в сфере финансовой кибербезопасности;
- формирование у будущих бакалавров представлений об основах технологий информационной безопасности в цифровой экономике;
- развитие у студентов навыков оценки качества, достаточности и надежности информации по контрагентам, ведение базы данных по клиентам в программном комплексе, составление аналитических заключений, рейтингов, прогнозов с целью предотвращения сделок с недобросовестными партнерами и поддерживания постоянных контактов с данными контрагентами.

2. Содержание дисциплины:

№ п/п	Наименование разделов / тем дисциплины
1.	**Раздел 1. Финансовые технологии в цифровой экономике.**
2.	Тема 1. Особенности информационных взаимодействий в финансовом секторе.
3.	Тема 2. Современные финансовые технологии. Цифровая трансформация финансовых услуг.
4.	Тема 3. Влияние цифровых технологий на развитие банковской сферы.
5.	Тема 4. Цифровизация страхового рынка.
6.	**Раздел 2. Финансовая кибербезопасность: общие положения.**
7.	Тема 5. Концепция (стратегия) национальной информационной безопасности Российской Федерации. Законодательство в сфере финансовой кибербезопасности.
8.	Тема 6. Современные угрозы в цифровом секторе.
9.	Тема 7. Финансовая кибербезопасность в РФ: угрозы и противодействие им.
10.	**Раздел 3. Киберпреступность и способы её предотвращения в финансовой сфере.**
11.	Тема 8. Преступления в сфере информационных технологий.
12.	Тема 9. Хакеры и проблемы обеспечения финансовой безопасности.
13.	Тема 10. Международное сотрудничество в сфере финансовой кибербезопасности.
Трудоемкость дисциплины составляет 4 з.е. / 144 часа	

Форма контроля – ***экзамен***

Составитель:
Доцент кафедры бухгалтерского учета и анализа
Краснодарского филиала РЭУ им. Г.В. Плеханова
И.Н. Колкарева