Приложение 6
к основной профессиональной образовательной программе
по направлению подготовки 38.03.01 Экономика
направленность (профиль) программы Финансовая безопасность

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

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ «ФИНАНСОВАЯ КИБЕРБЕЗОПАСНОСТЬ В ЦИФРОВОЙ ЭКОНОМИКЕ»

Направления подготовки 38.03.01 Экономика
Направленность (профиль) программы Финансовая безопасность

Уровень высшего образования Бакалавриат

Год начала подготовки - 2021г.

Краснодар – 2021 г.

Составитель:

к.ю.н., доцент, доцент И.Н. Колкарева

Оценочные средства одобрены на заседании кафедры бухгалтерского учета и анализа протокол № 6 от 28 января 2021 г.

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

по дисциплине «Финансовая кибербезопасность в цифровой экономике»

ПЕРЕЧЕНЬ КОМПЕТЕНЦИЙ С УКАЗАНИЕМ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ И ЭТАПОВ ИХ ФОРМИРОВАНИЯ ПО ДИСЦИПЛИНЕ

Формируемые компетенции (*код и наименование компетенции*)	**Индикаторы достижения компетенций (*код и наименование индикатора*)**	**Результаты обучения *(знания, умения)***	**Наименование контролируемых разделов и тем**
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.	Тема 1. Особенности информационных взаимодействий в финансовом секторе. Тема 2. Современные финансовые технологии. Цифровая трансформация финансовых услуг. Тема 3. Влияние цифровых технологий на развитие банковской сферы. Тема 5. Концепция (стратегия) национальной информационной безопасности Российской Федерации. Законодательство в сфере финансовой кибербезопасности. Тема 6. Современные угрозы в цифровом секторе. Тема 7. Финансовая кибербезопасность в РФ: угрозы и противодействие им. Тема 8. Преступления в сфере информационных технологий. Тема 9. Хакеры и проблемы обеспечения финансовой безопасности. Тема 10. Международное сотрудничество в сфере финансовой кибербезопасности.
	ПК-1.5 Организация и поддерживание постоянных контактов с рейтинговыми агентствами, аналитиками инвестиционных организаций, консалтинговыми организациями, аудиторскими организациями, оценочными фирмами, государственными и муниципальными	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	Тема 1. Особенности информационных взаимодействий в финансовом секторе. Тема 2. Современные финансовые технологии. Цифровая трансформация финансовых услуг. Тема 6. Современные угрозы в цифровом секторе. Тема 7. Финансовая кибербезопасность в РФ:

	органами управления, общественными организациями, средствами массовой информации,	профессиональной деятельности, получать, интерпретировать и документировать результаты исследований, владеть базовыми навыками работы на персональном компьютере.	угрозы и противодействие им. Тема 10. Международное сотрудничество в сфере финансовой кибербезопасности.

МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ХАРАКТЕРИЗУЮЩИЕ ЭТАПЫ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ

Перечень учебных заданий на аудиторных занятиях
Вопросы для проведения опроса обучающихся

Тема 1. Особенности информационных взаимодействий в финансовом секторе.
Индикатор достижения: *(ПК-1.2, ПК-1.5)*

1. Государственная информационная политика в сфере финансового контроля.
2. Информационное обеспечение государственного финансового контроля.
3. Информатизация деятельности в сфере финансового контроля Российской Федерации.
4. Автоматизированная информационная система «Финансы».
5. Государственная интегрированная информационная система управления бщественными финансами «Электронный бюджет».
6. Функциональная структура Общероссийского официального сайта государственных (муниципальных) закупок.
7. Автоматизированная информационная система Федеральной налоговой службы России (АИС ФНС).
8. Государственная информационная система о государственных и муниципальных платежах (ГИС ГМП).
9. Организация информационного взаимодействия Федерального казначейства РФ с органами внешнего финансового контроля.

Тема 2. Современные финансовые технологии. Цифровая трансформация финансовых услуг.
Индикатор достижения: *(ПК-1.2, ПК-1.5)*

1. Цифровые технологии в финансовой сфере: эволюция и основные тренды в России и за рубежом
2. Тенденции и тренды рынка финансовых инфо-коммуникационных технологий.
3. Место России на мировом рынке финтеха и показатели «технологического» проникновения на глобальном рынке.
4. Этапы внедрения fintech в финансово-кредитной сфере России.

Реферат

1. Цифровая трансформация финансовых услуг: модели развития и стратегии для участников отрасли.

2. Модели развития цифровизации финансовых услуг: американо-китайская, российская и европейская.

Тема 3. Влияние цифровых технологий на развитие банковской сферы.

Индикатор достижения: *(ПК-1.2, ПК-1.5)*

1. Перспективы развития fintech в банковской сфере.
2. Будущее банковского сектора России в условиях цифровизации.
3. Трансформация бизнес-модели в банковской отрасли.
4. Мероприятия банка России по цифровизации банковской системы.

Тема 4. Цифровизация страхового рынка.

Индикатор достижения: *(ПК-1.2. ПК-1.5)*

1. Сквозная цифровизация страхового рынка.
1. Направления цифровизации страхования.

1. Показатели цифровизации страхового рынка.
2. Практика цифровизации российского страхового рынка.
3. Приоритетные цифровые технологии по бизнес-процессам в страховых компаниях
4. Практика страхования рисков цифровой экономики
5. Перспективы развития цифрового страхования в России

Тема 5. Концепция (стратегия) национальной информационной безопасности Российской Федерации. Законодательство в сфере финансовой кибербезопасности.

Индикатор достижения: *(ПК-1.2, ПК-1.5)*

1. Теоретические основы защиты информации. Концепция информационной безопасности

2. Методологические принципы защиты информации.

3. Корпоративная политика информационной безопасности и защиты информации.

4. Состав и структура системы обеспечения информационной безопасности Российской Федерации (СОИБ РФ).

5. Основные элементы организационной основы СОИБ РФ. Силы обеспечения информационной безопасности РФ.

6. Законодательство в сфере финансовой кибербезопасности.

7. Глобальное управление в сфере кибербезопасности: взгляд с позиции международного права и права ЕС.

Реферат, презентация

1. Концепция (стратегия) национальной информационной безопасности РФ.

2. Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы".

3. Стратегия экономической безопасности Российской Федерации на период до 2030 года.

Тема 6. Современные угрозы в цифровом секторе.

Индикатор достижения: *(ПК-1.2, ПК-1.5)*

1. Риски кибербезопасности при удаленной работе.
2. Развитие интернета вещей.
3. Рост количества программ-вымогателей.
4. Увеличение количества облачных сервисов и угроз безопасности облачной инфраструктуры.
5. «Умные» атаки социальной инженерии.
6. Конфиденциальность данных как дисциплина.
7. Совершенствование многофакторной аутентификации.
8. Активный рост искусственного интеллекта
9. Мобильная кибербезопасность.
10. Развитие инсайдерских угроз.

Тема 7. Финансовая кибербезопасность в РФ: угрозы и противодействие им

Индикатор достижения: *(ПК-1.2, ПК-1.5)*

1. Финансовые потери клиентов (потребителей финансовых услуг), подрывающие доверие к современным финансовым технологиям.
2. Финансовые потери отдельных финансовых организаций, способные оказать существенное негативное (критическое) воздействие на их финансовое положение.
3. Нарушение операционной надежности и непрерывности предоставления финансовых услуг, приводящее к репутационному ущербу и нарастанию социальной напряженности в обществе.
4. Развитие системного кризиса в случае возникновения инцидентов информационной безопасности вследствие кибератак в значимых для финансового рынка организациях.

Тема 8. Преступления в сфере информационных технологий.

Индикатор достижения: *(ПК-1.2. ПК-1.5)*

1. Уголовно-правовая характеристика преступлений, совершенных с использованием информационных, коммуникационных технологий и в сфере компьютерной информации.
2. Особенности квалификации преступлений, совершенных с использованием информационно-коммуникационных технологий и в сфере компьютерной информации.
3. Система противодействия преступлениям, совершенным с использованием информационно-коммуникационных технологий и в сфере компьютерной информации.
4. Предупреждение преступлений, совершаемых с использованием информационно-коммуникационных технологий и в сфере компьютерной информации.

Тема 9. Хакеры и проблемы обеспечения финансовой безопасности.

Индикатор достижения: *(ПК-1.2. ПК-1.5)*

1. История хакерских методов.
2. Хакерские атаки.
3. Хакеры и хактивизм в условиях цифровой экономики.

ЗАДАНИЯ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ

Примерная тематика презентаций. Задачи.

Индикатор достижения: *(ПК-1.2. ПК-1.5)*

Задача 1.

Иванов осуществлял рассылку электронных писем клиентам банка Роспромторгбанк, содержащих информацию о поступлении на их счет призовой суммы, полученной в результате выигрыша в лотерее, проводимой банком. Для получения денежных средств клиентам необходимо было пройти по Интернет-ссылке, указанной в письме, подтвердить свои персональные данные и согласие на получение выигрыша. Однако, указанный в письмах электронный адрес банка приводил на сайт-дублёр, созданный Ивановым. В результате противоправных действий Иванова, несколько человек, зашедших на этот сайт, указали свои данные. Иванов, используя персональные данные клиентов, перевел с их счетов все имеющиеся денежные средства, в общей сумме один миллион восемьсот тысяч рублей. Квалифицируйте содеянное Ивановым. Определите, имеются ли в его действиях признаки множественности преступлений.

Задача 2.

Студенты факультета бухгалтерского учета и аудита в целях срыва тестирования для проверки остаточных знаний по дисциплине, изучаемой ими в прошлом году, запустили в компьютерную сеть аудитории, где планировалось тестирование, вредоносную компьютерную программу. Их действия повлекли нарушения в работе компьютерной системы на факультете и уничтожение базы тестов. Как квалифицировать их действия?

Реферат, презентация

1. Определение мотивации хакеров.
2. Романтизация хакерского движения: киберпанк.
3. Киберпреступность в информационном обществе: хакеры «белые», «чёрные» и «серые».

Задача 1. Когда новый сотрудник случайно загрузил вредоносную программу, в сторонней службе управления персоналом компании «Нева» произошла утечка данных. Информация о персонале компании похищена. Кто несет ответственность за это?

Задание. Возникла следующая ситуация. Во всплывающем окне на рабочем столе сообщается, что для загруженного надежного приложения по проверке правописания доступно новое обновление. Как поступить в данной ситуации правильно?

Тема 10. Международное сотрудничество в сфере финансовой кибербезопасности.

Индикатор достижения: *(ПК-1.2, ПК-1.5)*

1. Развитие международного сотрудничества в области обеспечения информационной безопасности

2. Международные организации в области информационной безопасности.

3. Правовое регулирование сети Интернет.

4. Региональное и двустороннее сотрудничество России в сфере обеспечения информационной безопасности.

5. Взаимодействие государств по созданию системы международной информационной безопасности.

6. Ассоциация аудита и контроля информационных систем – ISACA: общая характеристика.

7. Центр интернет-безопасности – CIS.

6 Критерии оценки:

0,5 балла выставляется обучающемуся, если он свободно отвечает на теоретические вопросы и показывает глубокие знания изученного материала,

0,4 балла выставляется обучающемуся, если его ответы на теоретические вопросы не достаточно полные, имеются ошибки при ответах на дополнительные вопросы,

0,3 балла выставляется обучающемуся, если он отвечает на 50% задаваемых вопросов и частично раскрывает содержание дополнительных вопросов,

0,2 балла выставляется обучающемуся, если он теоретическое содержание курса освоил частично или отсутствует ориентация в излагаемом материале, нет ответов на задаваемые дополнительные вопросы.

Задания для текущего контроля

Тестовые задания

Индикатор достижения: (ПК-1.2, ПК-1.5)

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.

11. 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

12.Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?
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

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

г) Руководство

14.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.

15. Предмет правового обеспечения кибербезопасности представляет собой:
а) совокупность общественных отношений, на которые направлено правовое воздействие в целях недопущения, выявления и пресечения проявлений угроз объектам национальных интересов в информационной сфере, а также минимизации негативных последствий проявления этих угроз;
б) совокупность общественных отношений, на которые направлено правовое воздействие только в целях недопущения проявлений угроз объектам национальных интересов в информационной сфере;
в) нет верного ответа.

16. Правовое обеспечение безопасности информации в форме сведений образуется:
а) совокупностью норм и институтов, регулирующих отношения по поводу только объекта - сведений, обладателем которых является субъект права;
б) совокупностью норм и институтов, регулирующих отношения по поводу следующих объектов: сведения, обладателем которых является субъект права; свобода мысли; субъективная значимость национальных культурных ценностей;
в) совокупностью норм и институтов, регулирующих отношения по поводу только объекта - свобода мысли.

17. Правовое обеспечение безопасности информации в форме сообщений определяется:
а) совокупностью норм и институтов, регулирующих отношения по поводу следующих объектов: сведения, обладателем которых является субъект права; свобода мысли; субъективная значимость национальных культурных ценностей;
б) совокупностью правовых норм и институтов, регулирующих отношения, объектами которых являются сообщения, передаваемые по каналам связи, данные, накапливаемые и обрабатываемые в информационных системах, автоматизированных системах управления, а также документы как входящие, так и не входящие в информационные системы;
в) совокупностью правовых норм и институтов, регулирующих отношения, объектами которых являются средства связи, автоматизации обработки информации, информационно-телекоммуникационные системы и средства массовой информации;
г) совокупностью правовых норм и институтов.

18. Содержание и структура законодательства в области информационной безопасности включает:
а) Конституция Российской Федерации - Нормативно-правовые акты (Указы) Президента Российской Федерации - Подзаконные акты Правительства Российской Федерации - Федеральные законы - Кодексы;
б) Конституция Российской Федерации - Нормативно-правовые акты (Указы) Президента Российской Федерации;
в) Подзаконные акты Правительства Российской Федерации - Федеральные законы - Кодексы;
г) нет верного ответа.

19. Законодательство Российской Федерации об информации, информационных технологиях и о защите информации состоит из:

а) Федерального закона «Об информации, информационных технологиях и о защите информации» и других федеральных законов, регулирующих отношения в области использования информации;
б) Федерального закона «О персональных данных» и других федеральных законов, регулирующих отношения в области использования информации;
в) Федерального закона «О коммерческой тайне» и других федеральных законов, регулирующих отношения в области использования информации;
г) Федерального закона «О государственной тайне» и других федеральных законов, регулирующих отношения в области использования информации.

20. **К общедоступной информации относятся:**

а) общеизвестные сведения и иная информация, доступ к которой не ограничен после достижения определенного возраста;
б) общеизвестные сведения и иная информация, доступ к которой не ограничен;
в) нет верного ответа.

21. Различают следующие виды информационных систем:

а) государственные информационные системы, муниципальные информационные системы, иные информационные системы;
б) государственные информационные системы; в) муниципальные информационные системы; г) нет верного ответа.

22. Правовой режим информационных технологий включает:

а) порядок регулирования использования информационно- коммуникационных сетей;
б) перечень областей государственного регулирования в сфере применения информационных технологий;
в) требования к государственным информационным системам; г) верны все варианты.

23. Защита информации представляет собой принятие правовых, организационных и технических мер, направленных:

а) на обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
б) соблюдение конфиденциальности информации ограниченного доступа; в) реализацию права на доступ к информации;
г) верны все варианты.

24. В структуру государственной системы защиты кибербезопасности РФ входят:

а) ФСБ РФ;
б) МВД РФ; в) ФСТЭК; г) ФСИН

25. Разделение информации на категории свободного и ограниченного доступа, причем информации ограниченного доступа подразделяются на:

а) отнесенные к государственной тайне;
б) отнесенные к служебной тайне (информации для служебного пользования), персональные данные (и другие виды тайн);
в) отнесенные к информации о прогнозах погоды; г) все верны ответы.

26. Государственная тайна — это:

а) защищаемые государственные сведения в области военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которой может нанести ущерб безопасности Российской Федерации;

б) защищаемые государственные сведения только в области военной и внешнеполитической деятельности, распространение которой может нанести ущерб безопасности Российской Федерации;
в) защищаемые государственные сведения только в области экономической и разведывательной деятельности, распространение которой может нанести ущерб безопасности Российской Федерации.

27. Гриф секретности — это:
а) реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе кроме сопроводительной документации на него;
б) реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него.
в) оба варианта верны.

28. Степень секретности — это:
а) категория, характеризующая важность такой информации, возможный ущерб в случае ее разглашения, степень ограничения доступа к ней и уровень ее охраны государством;
б) категория, характеризующая важность такой информации, возможный ущерб в случае ее разглашения, но не степень ограничения доступа к ней и уровень ее охраны государством;
в) нет верного ответа.

29. Срок засекречивания сведений, составляющих государственную тайну, не должен превышать:
а) 30 лет;
б) 40 лет;
в) 50 лет;
г) 60 лет.

30. Персональные данные - это:
а) конкретная информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных);
б) любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных);

в) любая информация, относящаяся к определенному или определяемому на основании такой информации юридическому лицу (субъекту персональных данных).

31. **ИСПДн согласно 5 пункту Постановления №1119 подразделяются на следующие группы (категории):**
а) Специальные ИСПДн;
б) Биометрические ИСПДн;
в) Общедоступные ИСПДн;
г) Иные ИСПДн;
д) верны все варианты.

32. Программа, осуществляющая несанкционированные действия по сбору, и передаче информации злоумышленнику, а также ее разрушение или злонамеренную модификацию.
Ответ: _____

33. Процесс преобразования информации, хранящейся в файле к виду, при котором уменьшается избыточность в ее представлении и соответственно требуется меньший объем памяти для ее хранения.

Ответ: _____

34. Какую задачу решает сертификация средств защиты информации?

а) обеспечения требуемого качества защиты информации;
б) повышения квалификации разработчиков средств защиты информации;
в) создания надежных средств защиты информации;
г) защиты отечественных производителей средств защиты информации.

35. Какие задачи решает система антивирусной защиты?

а) предотвращения проникновения вирусов к персональным ресурсам;
б) повышения надежности работы программного обеспечения;
в) предотвращения поломок технических средств;
г) повышения эффективности работы программных средств.

36. Что служит мерой опасности незаконного канала передачи информации?

а) пропускная способность незаконного канала
б)количество информации, передаваемой по незаконному каналу
в) время существования незаконного канала
г) число лиц, имеющих доступ к незаконному каналу

37. Какие шифры называются послойными?

а) состоящие из слоев шифрования;
б) состоящие из цепочки циклов шифрования;
в) выполняющие единственное преобразование информационного сообщения;
г) обеспечивающие высокоэффективное шифрование.

38. Какой цифровой документ подтверждает соответствие между открытым ключом и информацией, идентифицирующей владельца ключа?

а) код пользователя
б) цифровой сертификат
в) доверенность
г) шифр программы

39. Какой уровень контроля достаточен для ПО, используемого при защите информации с грифом «СС»?

а) первый
б) второй
в) третий
г) четвертый

40. Как используются дизассемблеры при взломе программы?

а) с их помощью изучается полученный код программы
б) с их помощью совершенствуется программное обеспечение
в) с их помощью кодируется программное обеспечение
г) они применяются для стыковки отдельных модулей

41. Кем формулируются требования к системе по защите цифровой информации?

а) разработчиком
б) пользователем
в) заказчиком
г) головной организацией

42. Что принято называть утечкой информации?

а) доступ посторонних лиц к конфиденциальной информации
б) выход информации, составляющей коммерческую тайну, за пределы области ее обращения

в) утрату информации, хранящейся на носителях

43. В чем заключается сущность приема "Асинхронная атака"?

а) это способ смешивания двух или более различных программ, поочередно выполняемых в памяти компьютера, что позволяет достигать любых целей - заложенных преступником

б) это способ размещения памяти компьютера двух или более различных программ, выполняемых одновременно

в) это способ смешивания двух или более различных программ, одновременно выполняемых в памяти компьютера, что позволяет достигать любых целей - заложенных преступником

44. Вредоносные программы - это

а) шпионские программы

б) программы, наносящие вред данным и программам, находящимся на компьютере

в) программы, наносящие вред пользователю, работающему на зараженном компьютере

г) троянские утилиты и сетевые черви

45. Вирус, поражающий документы называется

а) троян

б) файловый вирус

в) макровирус

г) сетевой червь

46. Открытым текстом в криптографии называют:

а) расшифрованный текст

б) любое послание

в) исходное послание

47. Шифрование – это:

а) процесс создания алгоритмов шифрования

б) процесс сжатия информации

в) процесс криптографического преобразования информации к виду, когда ее смысл полностью теряется

48. Аутентификацией называют:

а) процесс регистрации в системе

б) способ защиты системы

в) процесс распознавания и проверки подлинности заявлений о себе пользователей и процессов

49. К биометрической системе защиты относятся:

а) защита паролем

б) физическая защита данных

в) антивирусная защита

г) идентификация по радужной оболочке глаз

д) идентификация по отпечаткам пальцев

50. Компьютерные вирусы – это:

а) Вредоносные программы, наносящие вред данным.

б) Программы, уничтожающие данные на жестком диске

в) Программы, которые могут размножаться и скрыто внедрять свои копии в файлы, загрузочные сектора дисков, документы.

г) Программы, заражающие загрузочный сектор дисков и препятствующие загрузке компьютера

д) Это скрипты, помещенные на зараженных интернет-страничках

51. Отметьте составные части современного антивируса

а) модем

б) принтер

в) сканер

г) межсетевой экран
д) монитор

52. К вредоносным программам относятся:

а) потенциально опасные программы
б) вирусы, черви, трояны
в) шпионские и рекламные программы
г) вирусы, программы-шутки, антивирусное программное обеспечение
д) межсетевой экран, брандмауэр

53. Каким образом должен быть организован процесс формирования и потребления информации, составляющей коммерческую тайну предприятия?

а) он должен быть организован таким образом, чтобы исключить утечку информации
б) он должен быть организован таким образом, чтобы область обращения информации, была бы минимальна и достаточна
в) он должен быть организован таким образом, чтобы обеспечить сохранность информации

54. Какой из методов защиты информации на персональном компьютере или рабочей станции сети является основным?

а) шифрование с достаточной длиной ключа
б) средства антивирусной защиты
в) системы защиты, блокирующие загрузку компьютера до предъявления электронного идентификатора.

55. Понятие кибербезопасности включает в себя заботу о сохранности не только данных, но и душевного спокойствия пользователя интернета. Однако пока слабо развита защита от этой формы социальной провокации в сетевом общении. О чем идет речь?

а) Фаббинг;
б) Блоггинг;
в) Хактивизм;
г) Троллинг.

56. Разработчики вируса WannaCry явно поставили перед собой цель довести до слез любого, кто станет жертвой его беспощадной атаки, самой масштабной в истории. В чем принцип работы этого вируса?

а) при заражении этим вирусом на мониторе компьютера появляется видео с плачущим младенцем.
б) вирус заставляет зараженные компьютеры подключаться к определенным сайтам в определенные дни.
в) это вирус-шифровальщик, который требует за разблокировку данных выкуп в кибервалюте.
г) это компьютерный червь, который позволяет дистанционно управлять зараженным компьютером.

57. В некоторых европейских странах в целях борьбы с кибератаками вводится специальная сертификация для больших компаний. Какие средства необходимо использовать для того, чтобы подтвердить защищенность продукта от основных киберугроз?

а) Файервол
б) Средства контроля доступа пользователей
в) Патч-менеджмент

58. Кибербезопасность — это постоянная гонка вооружений, своеобразное соревнование между хакерами и специалистами по системам защиты информации. По прогнозам исследователей, развитие каких технологий приведет к возникновению абсолютно безопасной коммуникации?

а) Темные паттерны;

б) Облачные вычисления;
в) Квантовый компьютер;
г) Системы прокси-серверов.

59. В 1988 году аспирант Университета Корнелл, движимый любопытством, предпринял попытку измерить, насколько большим является интернет. Но все вышло из-под контроля, и его эксперимент стал одной из самых известных кибератак в истории. Какой вирус он создал?

а) Вирус Brain
б) Чернобыльский вирус
в) «Червь Морриса»
г) LOVELETTER-вирус.

60. В любом ПО есть уязвимые места, поэтому для обнаружения техник взломов нужны новые решения. Система определения нормального компьютерного поведения и обнаружения аномалий в нем — это основа кибербезопасности. Кто впервые ввел понятие «выявление аномалий»?

а) Дороти Деннинг
б) Алан Тьюринг
в) Линус Торвальдс
г) Бьёрн Страуструп.

Критерии оценки:

0,5 балла выставляется студенту, при условии его правильного ответа не менее чем на 90% тестовых заданий,

0,3 балла выставляется студенту при условии его правильного ответа от 70 до 89% тестовых заданий,

0,2 балла выставляется студенту при условии его правильного ответа от 50 до 69% тестовых заданий,

0,1 балл выставляется студенту при условии его правильного ответа менее чем на 50% тестовых заданий.

Формы заданий для творческого рейтинга

Индивидуальный проект

Индикатор достижения: (ПК-1.2, ПК-1.5)

Примерный перечень тем для написания индивидуального проекта:

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.
10. Основные сегменты цифровой стратегии банка.

11. Проблемы и перспективы цифровой трансформации российских банков.

12. Двойственный подход к цифровому страхованию.

13. Интернетизация страхового рынка.

14. Концепция (стратегия) национальной информационной безопасности РФ.

15. Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы".

16. Стратегия экономической безопасности Российской Федерации на период до 2030 года.

17. Обеспечение готовности кредитно-финансовой сферы гарантировать финансовую стабильность и операционную надежность в условиях реализации компьютерных атак.

18. Обеспечение операционной надежности и непрерывности предоставления финансовых и банковских услуг;

19. Контроль показателей риска реализации информационных угроз.

20. Контроль уровня банковских и финансовых операций, совершенных без согласия клиентов.

21. Мониторинг, оперативное реагирование и предотвращение компьютерных атак на организации кредитно-финансовой сферы.

22. Защита прав потребителей финансовых услуг через мониторинг показателей уровня финансовых потерь.

23. Содействие развитию инновационных финансовых технологий в части контроля показателей риска реализации информационных угроз и обеспечение необходимого уровня информационной безопасности.

24. Понятие и виды преступлений, совершаемых с использованием информационных технологий по действующему российскому уголовному законодательству.

25. Квалификация преступлений, совершаемых с использованием информационных технологий при множественности преступлений, при неоконченном преступлении, при соучастии.

26. Романтизация хакерского движения: киберпанк.

27. Киберпреступность в информационном обществе: хакеры «белые», «чёрные» и «серые».

28. Особенности информационных взаимодействий в финансовом секторе.

29. Цифровая трансформация финансовых услуг: модели развития и стратегии для участников отрасли.

30. Модели развития цифровизации финансовых услуг: американо-китайская, российская и европейская.

31. Электронные носители информации в уголовном судопроизводстве.

32. Определение мотивации хакеров.

33. Архитектура сетевой безопасности и управление процессом обеспечения безопасности.

34. Международные организации по кибербезопасности.

35. Национальные рамки кибербезопасности.

Критерии оценки:

5 баллов – выставляется обучающемуся, если выполнены все требования к написанию реферата (презентации): обозначена проблема и обоснована ее актуальность, проведен анализ различных точек зрения на рассматриваемую проблема и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объем,

соблюдены требования к внешнему оформлению, выполнена качественная презентации, оригинальность реферата -50%.

3 балла – выставляется обучающемуся, если основные требования к реферату (презентации): выполнены, но присутствуют недочеты. В частности, имеются неточности в изложении материала, отсутствует логическая последовательность в суждениях, не выдержан объем реферата, имеются упущения в оформлении презентации, оригинальность реферата -50%.

2 балла – выставляется обучающемуся, если имеются существенные отклонения от требований к реферату (презентации). В частности, тема раскрыта частично, допущены ошибки и отсутствуют выводы. Оригинальность реферата - 40%.

Анализ кейс-ситуации по теме 6. Современные угрозы в цифровом секторе
Задача 1.

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?

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.

Задача 3.

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?

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.

Критерии оценки:

- *0,5 балла студент проявляет глубокие знания и навыки, аналитические способности, творческий подход, аргументирует собственное мнение, демонстрирует зрелость суждений, самостоятельное мышление;*
- *0,4 балла - студент проявляет достаточный уровень знаний, навыков в оценке профессиональной ситуации, демонстрирует самостоятельность, но допускает некоторые неточности, отсутствует достаточная глубина и зрелость суждений;*
- *0,3 балла - студент отвечает не достаточно глубоко и самостоятельно, уровень знаний и сформированности компетенций не высокий, либо отсутствует конкретность, ясность и четкость ответа;*
- *0,2 балла - студент отвечает неуверенно, поверхностно и бессистемно, допускает неточности и ошибки.*

МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ХАРАКТЕРИЗУЮЩИЕ ЭТАПЫ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ ВО ВРЕМЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Структура экзаменационного задания по дисциплине «Финансовая кибербезопасность в цифровой экономике»

Наименование оценочного материала	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*

Задания, включаемые в экзаменационное задание

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.

Вопросы 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.

Номер вопроса	Перечень вопросов к экзамену
15.	Защита информации при использовании технологии big data в информационных системах и технологиях управления бизнес-процессами.
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.
38.	Риск разглашения конфиденциальной информации.
39.	Мониторинг, прогнозирование и планирование предупреждения цифровой преступности.
40.	Предупреждение преступлений, совершаемых в условиях цифровой

Номер вопроса	Перечень вопросов к экзамену
	трансформации.
41.	Информационное обеспечение финансовой безопасности банка.
42.	Кибератаки на кредитные организации.
43.	Защита национальных и финансовых интересов России в международных экономических и финансовых организациях.
44.	Рейтинговая оценка при диагностике финансовой безопасности.
45.	Оценка эффективности системы защиты объекта.
46.	Анализ риска финансовой безопасности.
47.	Классификация угроз финансовой безопасности и рисков.
48.	Устойчивость банковской системы как элемент системы экономической безопасности страны.
49.	Основные понятия в области кибербезопасности Интернета вещей;
50.	Кибербезопасность для систем «Умного города».

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	**Знает верно и в полном объеме:** основы социологии, психологии, технологии проведения социологических и маркетинговых исследований **Умеет верно и в полном объеме:**	

			организациями, аудиторскими организациями, оценочными фирмами, государственными и муниципальными органами управления, общественными организациями, средствами массовой информации, информационными, рекламными агентствами.	работать в автоматизированных системах информационного обеспечения профессиональной деятельности, получать, интерпретировать и документировать результаты 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 организациями, аудиторскими организациями, оценочными фирмами, государственными и муниципальными органами управления, общественными организациями, средствами массовой информации, информационными, рекламными агентствами.	**Знает с незначительными замечаниями:** основы социологии, психологии, технологии проведения социологических и маркетинговых исследований **Умеет с незначительными замечаниями:** работать 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	**Базовый**

				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.	**Знает на базовом уровне:** основы социологии, психологии, технологии проведения социологических и 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	**Компетенции не сформированы**

				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.	
			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.	**Не знает на базовом 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.	