



Федеральное государственное образовательное бюджетное учреждение высшего образования
«ФИНАНСОВЫЙ УНИВЕРСИТЕТ ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»
(Финансовый университет)

Кафедра информационной безопасности
Факультет информационных технологий и анализа больших данных

Документ подписан усиленной неквалифицированной электронной подписью.

Организация: «ФИНАНСОВЫЙ УНИВЕРСИТЕТ ПРИ ПРАВИТЕЛЬСТВЕ
РОССИЙСКОЙ ФЕДЕРАЦИИ»

Сертификат: ohNjJR1FGQIL+IsREhYIqCIDZ/zy/vi0

Утверждено: Проректор по учебной и методической работе, Е.А. Каменева

Дата: 06.05.2026 г.

А.Н. Когтева
Кибербезопасность в сфере финансов

Рабочая программа дисциплины
для студентов, обучающихся по направлению подготовки
38.03.01 - Экономика,
Образовательная программа «Финансы и искусственный интеллект»
Профиль:
«Финансы и искусственный интеллект»

Рекомендовано
Факультет информационных технологий и анализа больших данных
(протокол № 09 от 16.06.2026 г.)

Одобрено
Кафедра информационной безопасности
(протокол № 8 от 09.06.2026 г.)



Содержание

1. Наименование дисциплины	3
2. Перечень планируемых результатов освоения образовательной программы (перечень компетенций) с указанием индикаторов их достижения и планируемых результатов обучения по дисциплине	3
3. Место дисциплины в структуре образовательной программы	7
4. Объем дисциплины (модуля) в зачетных единицах и в академических часах с выделением объема аудиторной (лекции, семинары) и самостоятельной работы обучающихся	7
5. Содержание дисциплины, структурированное по темам (разделам) дисциплины с указанием их объемов (в академических часах) и видов учебных занятий	8
5.1. Содержание дисциплины	8
5.2. Учебно – тематический план	10
5.3. Содержание семинаров, практических занятий	11
6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине	13
6.1. Перечень вопросов, отводимых на самостоятельное освоение дисциплины, формы внеаудиторной самостоятельной работы	13
6.2. Перечень вопросов, заданий, тем для подготовки к текущему контролю	15
7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине	16
8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	7
9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины	8
10. Методические указания для обучающихся по освоению дисциплины	32
11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень необходимого программного обеспечения и информационных справочных систем (при необходимости)	33
12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине	33



1. Наименование дисциплины

Кибербезопасность в сфере финансов

2. Перечень планируемых результатов освоения образовательной программы (перечень компетенций) с указанием индикаторов их достижения и планируемых результатов обучения по дисциплине

Код компетенции	Наименование компетенции	Индикаторы достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции
ПКН-3	Способность осуществлять сбор, обработку и статистический анализ данных, применять математические методы для решения стандартных профессиональных финансово-экономических задач, интерпретировать полученные результаты	Проводит сбор, обработку и статистический анализ данных для решения финансово-экономических задач	Знать: основы обеспечения безопасности объектов информатизации прикладного уровня в организациях кредитно-финансовой сферы (далее - КФС) Уметь: вносить предложения об изменении контрольных показателей уровня рисков информационной безопасности в организациях КФС.
		Формулирует математические постановки финансово-экономических задач, переходит от экономических постановок задач к математическим моделям.	Знать: принципы обеспечения операционной надежности (киберустойчивости) в организациях КФС. Уметь: осуществлять выбор организационных и технических мер защиты информации и обеспечения операционной надежности (киберустойчивости) в организациях КФС.
		Системно подходит к выбору математических методов и информационных технологий для решения конкретных финансово-экономических задач в профессиональной области.	Знать: основы обеспечения безопасности объектов информатизации прикладного уровня в организациях КФС. Уметь: разрабатывать предложения по совершенствованию методологии обеспечения операционной надежности (киберустойчивости) в организациях КФС.



Код компетенции	Наименование компетенции	Индикаторы достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции
		Анализирует результаты исследования математических моделей финансово-экономических задач и делает на их основании количественные и качественные выводы и рекомендации по принятию финансово-экономических решений.	Знать: Специфика платежных процессов в организациях КФС Уметь: Применять организационные и технические меры обеспечения операционной надежности (киберустойчивости) в организациях КФС
ПKN-4	Способность оценивать показатели деятельности экономических субъектов	Проводит анализ внешней и внутренней среды ведения бизнеса, выявляет основные факторы экономического роста, оценивает эффективность формирования и использования производственного потенциала экономических субъектов.	Знать: угрозы безопасности информации, в том числе безопасности персональных данных, в автоматизированных системах в организациях КФС. Уметь: планировать и организовывать контроль выполнения организационных технических мер по защите информации, в том числе по защите персональных данных, в организациях КФС.
		Рассчитывает и интерпретирует показатели деятельности экономических субъектов.	Знать: принципы целеполагания, виды и методы организационного планирования. Уметь: устанавливать и поддерживать деловые контакты, связи, отношения с сотрудниками и заинтересованными сторонами по вопросам управления рисками информационной безопасности, обеспечения информационной безопасности и операционной надежности (киберустойчивости) в организациях КФС.
ПКП-2	Способность осуществлять мониторинг экономических,	Грамотно использует достоверные источники финансово-экономиче-	Знать: законодательство Российской Федерации, нормативные правовые акты, национальные, межгосударствен-



Код компетенции	Наименование компетенции	Индикаторы достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции
	промышленных и корпоративных изменений посредством анализа информации и интерпретировать данные, связанные с финансовыми решениями, включая цены, прибыль, устойчивость, дальнейшие перспективы в плане инвестиционных рисков и экономического влияния, применяя возможности инновационных финансовых технологий	ской и статистической информации для сбора, обработки и анализа данных с целью дальнейшего использования в решении экономических и финансовых задач.	ные и международные стандарты в области защиты информации. Уметь: планировать политику безопасности компонентов (операционных систем, баз данных, компьютерных сетей, программных систем) автоматизированной системы в организациях кредитно-финансовой сферы.
		Применяет математические методы и информационные технологии проведения мониторинга экономических показателей, рассчитанных на основе данных, связанных с финансовыми решениями	Знать: правила сбора и регистрации информации об инцидентах информационной безопасности в организациях кредитно-финансовой сферы (далее по тексту - КФС). Уметь: анализировать и применять методологическую базу, требования законодательства Российской Федерации, нормативных актов Банка России, международных и национальных стандартов в области защиты информации, обеспечения информационной безопасности, управления рисками информационной безопасности в организациях КФС, а также обнаружения, предупреждения и ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры организаций КФС, и реагирования на компьютерные инциденты.
		Проводит оценку инвестиционных рисков и экономического влияния на основе полученных данных и проведенного анализа.	Знать: Руководящие и методические документы уполномоченных федеральных органов исполнительной власти, нормативные акты Банка России в области защиты информации, обеспечения информационной безопасности, управления рисками информационной безопасности в ор-



Код компетенции	Наименование компетенции	Индикаторы достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции
			ганизациях КФС, а также в области обнаружения, предупреждения и ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры, реагирования на компьютерные инциденты Уметь: Осуществлять работу с техническими средствами защиты информации и системами, реализующими функции управления инцидентами информационной безопасности организаций КФС



3. Место дисциплины в структуре образовательной программы

Дисциплина «Кибербезопасность в сфере финансов» относится к «Профилю "Финансы и искусственный интеллект"».

4. Объем дисциплины (модуля) в зачетных единицах и в академических часах с выделением объема аудиторной (лекции, семинары) и самостоятельной работы обучающихся

очно-заочная форма обучения

Вид учебной работы по дисциплине	Всего (в з/е и часах)	Семестр 8 (в часах)
Общая трудоемкость дисциплины	4/144	144
<i>Контактная работа – Аудиторные занятия</i>	<i>32</i>	<i>32</i>
<i>Лекции</i>	<i>4</i>	<i>4</i>
<i>Семинары, практические занятия</i>	<i>28</i>	<i>28</i>
<i>Самостоятельная работа</i>	<i>112</i>	<i>112</i>
Вид текущего контроля	Контрольная работа	Контрольная работа
Вид промежуточной аттестации	Экзамен	Экзамен



5. Содержание дисциплины, структурированное по темам (разделам) дисциплины с указанием их объемов (в академических часах) и видов учебных занятий

5.1. Содержание дисциплины

Тема 1. Задачи и основные направления деятельности Банка России в области информационной безопасности.

Правовое регулирование. Закон о НПС. Закон о персональных данных. Нормативные документы Банка России в части защиты информации. Нормативные документы ФСТЭК. Постановления Правительства РФ. Нормативные документы ФСБ России. Стандарты в области обеспечения безопасности. Стандарты оценки систем защиты и защищенности автоматизированных систем Обеспечение информационной безопасности и киберустойчивости инфраструктуры. Обеспечение информационной безопасности и киберустойчивости прикладного программного обеспечения. Обеспечение информационной безопасности и киберустойчивости технологий обработки данных. Обеспечение информационной безопасности и киберустойчивости финансовых технологий. Подготовка кадров и обеспечение доверия граждан к цифровой среде. Международное сотрудничество. Национальная программа «Цифровая экономика Российской Федерации». Центр компетенций по обеспечению информационной безопасности и противодействию кибератакам в кредитно-финансовой сфере. Надзорная деятельность.

Тема 2. Кибербезопасность в условиях применения дистанционного банковского обслуживания.

Механизм построения кибербезопасности в банковской сфере. Методология анализа рисков недостаточного обеспечения кибербезопасности. Информационное общество и кибербезопасность. Кибербезопасность в условиях развития интернета вещей и электронного банкинга. Типовые атаки на организации кредитно-финансовой сферы.

Тема 3. Оценка защищенности кредитно-финансовых систем.

Стандарты и методологии проверки и оценки защищенности ИТ и СУИБ: их отличия, сильные и слабые стороны. Международный стандарт оценки защищенности ISO/IEC 27004:2009 и ГОСТ Р ИСО/МЭК 27004-2011. Базовые вопросы проверки защищенности. Оценка эффективности и результативности деятельности по



управлению ИБ. Измерение, мера измерения, показатель и метрика. Метрики безопасности. Системы анализа защищенности.

Тема 4. Организация системы защиты информации кредитно-финансовых систем.

Архитектура информационной безопасности в кредитно-финансовой сфере. Прослеживаемые тенденции к распространению киберугроз. Реагирование на события информационной безопасности. Этапы построения системы защиты информации. Политика безопасности. Оценка эффективности инвестиций в информационную безопасность. Обеспечение компьютерной безопасности учетной информации. Обеспечение информационной безопасности автоматизированных банковских систем (АБС). Контур системы управления операционным риском. Состав системы управления ОР. Взаимодействие с поставщиками ИТ и облачных услуг. Подходы к регулированию аутсорсинга. Оперативная обработка событий риска.



5.2. Учебно – тематический план

Очно-заочная форма обучения

п/ п	Наименование тем (разделов) дисциплины	Трудоемкость в часах				
		Всего	Контактная работа - Аудиторная работа			Самостоятельная работа
			Общая, в т.ч.:	Лекции	Семинары, практические занятия	
1	Задачи и основные направления деятельности Банка России в области информационной безопасности.	36	8	1	7	28
2	Кибербезопасность в условиях применения дистанционного банковского обслуживания.	36	8	1	7	28
3	Оценка защищенности кредитно-финансовых систем.	36	8	1	7	28
4	Организация системы защиты информации кредитно-финансовых систем.	36	8	1	7	28
В целом по дисциплине		144	32	4	28	112



5.3. Содержание семинаров, практических занятий

Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
Задачи и основные направления деятельности Банка России в области информационной безопасности.	Закон о НПС. Закон о персональных данных. Нормативные документы Банка России в части защиты информации. Нормативные документы ФСТЭК. Постановления Правительства РФ. Нормативные документы ФСБ России. Стандарты в области обеспечения безопасности. Обеспечение информационной безопасности и киберустойчивости инфраструктуры. Обеспечение информационной безопасности и киберустойчивости прикладного программного обеспечения. Обеспечение информационной безопасности и киберустойчивости технологий обработки данных. Обеспечение информационной безопасности и киберустойчивости финансовых технологий.	Групповые дискуссии, доклады, презентации.
Кибербезопасность в условиях применения дистанционного банковского обслуживания.	Механизм построения кибербезопасности в банковской сфере. Методология анализа рисков недостаточного обеспечения кибербезопасности. Информационное общество и кибербезопасность. Кибербезопасность в условиях развития интернета вещей и электронного банкинга. Типовые атаки на организации кредитно-финансовой сферы.	Групповые дискуссии, доклады, презентации.



Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
Оценка защищенности кредитно-финансовых систем.	Стандарты и методологии проверки и оценки защищенности ИТ и СУИБ: их отличия, сильные и слабые стороны. Международный стандарт оценки защищенности ISO/IEC 27004:2009 и ГОСТ Р ИСО/МЭК 27004-2011. Базовые вопросы проверки защищенности. Оценка эффективности и результативности деятельности по управлению ИБ. Метрики безопасности. Системы анализа защищенности.	Групповые дискуссии, доклады, презентации.
Организация системы защиты информации кредитно-финансовых систем.	Этапы построения системы защиты информации. Политика безопасности. Оценка эффективности инвестиций в информационную безопасность. Обеспечение компьютерной безопасности учетной информации. Обеспечение информационной безопасности автоматизированных банковских систем (АБС). Контур системы управления операционным риском. Состав системы управления ОР. Взаимодействие с поставщиками ИТ и облачных услуг. Подходы к регулированию аутсорсинга.	Групповые дискуссии, доклады, презентации.



6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

6.1. Перечень вопросов, отводимых на самостоятельное освоение дисциплины, формы внеаудиторной самостоятельной работы

Наименование тем (разделов) дисциплины	Перечень вопросов, отводимых на самостоятельное освоение	Формы внеаудиторной самостоятельной работы
Задачи и основные направления деятельности Банка России в области информационной безопасности.	Подготовка кадров и обеспечение доверия граждан к цифровой среде. Международное сотрудничество. Национальная программа «Цифровая экономика Российской Федерации». Центр компетенций по обеспечению информационной безопасности и противодействию кибератакам в кредитно-финансовой сфере. Надзорная деятельность.	- работа с учебной, научной и справочной литературой; - конспект; - подготовка докладов по теме; - подготовка презентаций по теме
Кибербезопасность в условиях применения дистанционного банковского обслуживания.	Механизм построения кибербезопасности в банковской сфере. Методология анализа рисков недостаточного обеспечения кибербезопасности. Информационное общество и кибербезопасность. Кибербезопасность в условиях развития интернета вещей и электронного банкинга. Типовые атаки на организации кредитно-финансовой сферы.	- работа с учебной, научной и справочной литературой; - конспект; - подготовка докладов по теме; - подготовка презентаций по теме
Оценка защищенности кредитно-финансовых систем.	Международный стандарт оценки защищенности ISO/IEC 27004:2009 и ГОСТ Р ИСО/МЭК 27004-2011. Базовые вопросы проверки защищенности. Оценка эффективности и результативности деятельности по управлению ИБ. Измерение, мера измерения, показатель	- работа с учебной, научной и справочной литературой; - конспект; - подготовка докладов по теме; - подготовка презентаций по теме



Наименование тем (разделов) дисциплины	Перечень вопросов, отводимых на самостоятельное освоение	Формы внеаудиторной самостоятельной работы
	и метрика. Метрики безопасности. Системы анализа защищенности.	
Организация системы защиты информации кредитно-финансовых систем.	Этапы построения системы защиты информации. Политика безопасности. Оценка эффективности инвестиций в информационную безопасность.	- работа с учебной, научной и справочной литературой; - конспект; - подготовка докладов по теме; - подготовка презентаций по теме



6.2. Перечень вопросов, заданий, тем для подготовки к текущему контролю

Примерный перечень вопросов к контрольной работе:

1. Международные стандарты и лучшие практики оценки защищенности банковских систем.
2. Антропогенные уязвимости, риски и угрозы кибербезопасности.
3. Техногенные уязвимости, риски и угрозы кибербезопасности
4. Назначение и виды обрабатываемых данных в автоматизированной системе обработки бэк-офисных банковских операций.
5. Назначение и виды обрабатываемых данных, в автоматизированной системы обработки систем удаленного доступа к счетам физических лиц.
6. Особенности конкурентной разведки в Японии.
7. Конкурентная разведка в Германии.
8. Конкурентная разведка в Швеции.
9. Основные процедуры data mining в задачах финансовой разведки
10. Обнаружение признаков отмывания доходов в транзакциях
11. Обнаружение признаков кибератак
12. Преимущества data mining в конкурентной разведке.
13. Проблемы интерпретации результатов анализа
14. Бенчмаркинг и конкурентная разведка
15. Обеспечение кибербезопасности и киберустойчивости инфраструктуры.
16. Обеспечение информационной безопасности и киберустойчивости прикладного программного обеспечения.
17. Обеспечение информационной безопасности и киберустойчивости технологий обработки данных.
18. Обеспечение информационной безопасности и киберустойчивости финансовых технологий
19. Организация службы информационной безопасности автоматизированных банковских систем.
20. Организация контроля информационной безопасности в кадровых службах.

Дополнительная информация

Критерии балльной оценки различных форм текущего контроля успеваемости содержатся в соответствующих методических рекомендациях кафедры.



7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

Перечень компетенций с указанием индикаторов их достижения в процессе освоения образовательной программы содержится в разделе 2. «Перечень планируемых результатов освоения образовательной программы (перечень компетенций) с указанием индикаторов их достижения и планируемых результатов обучения по дисциплине».

Типовые контрольные задания или иные материалы, необходимые для оценки индикаторов достижения компетенций, умений и знаний

Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	Типовые контрольные задания
ПKN-3. Способность осуществлять сбор, обработку и статистический анализ данных, применять математические методы для решения стандартных про-	Проводит сбор, обработку и статистический анализ данных для решения финансово-экономических задач	Знать: основы обеспечения безопасности объектов информатизации прикладного уровня в организациях кредитно-финансовой сферы (далее - КФС) Уметь: вносить предложения об изменении контрольных показателей уровня рисков информацион-	Внесение предложений по изменению контрольных показателей рисков ИБ в организациях КФС — это аналитический процесс корректировки ключевых индикаторов риска и количественных показателей. Он базируется на мониторинге актуальных киберугроз и адаптации систем защиты к требованиям регуляторов. Выполните одно из заданий по теме: - Анализ текущих показателей: Оценка действующих сигнальных и контрольных пороговых значений по ключевым рискам - Обоснование изменений: Фиксация причин (изменение ландшафта угроз, рост числа инцидентов, внедрение новых ИТ-систем или изменение бизнес-процессов). - Разработка новых метрик: Предложение новых пороговых значений или добавление/исключение индикаторов, отражающих реальную вероятность реализации недопустимых событий



Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	Типовые контрольные задания
профессиональных финансово-экономических задач, интерпретировать полученные результаты		ной безопасности в организациях КФС.	Оценка эффективности: Прогноз того, как предлагаемые изменения повлияют на финансовую устойчивость организации и операционную надежность.
	Формулирует математические постановки финансово-экономических задач, переходит от экономических постановок задач к математическим моделям.	Знать: принципы обеспечения операционной надежности (киберустойчивости) в организациях КФС. Уметь: осуществлять выбор организационных и технических мер защиты информации и обеспечения операционной надежности (киберустойчивости) в организациях КФС.	Выполните одно из заданий: 1. Составьте перечень из 3 обязательных технических и 3 организационных мер, которые необходимо внедрить для соответствия Положению Банка России № 757-П. Обоснуйте свой выбор. 2. Руководствуясь Положением Банка России № 850-П, определите сигнальное и контрольное значения показателя операционной надежности. Укажите максимально допустимое время простоя системы и выберите две технические меры (например, резервирование узлов), которые обеспечат заданную непрерывность. 3. Выберите комплекс из трех технических мер, направленных на предотвращение развития атаки, и обоснуйте их применение в контуре КФС. 4. Проведите сравнительный анализ двух актуальных российских DLP-систем (например, «СёрчИнформ КИБ» или «Solar Dozor»). Выберите одну из них, опираясь на требования регуляторов к обеспечению операционной надежности и защиты информации, укажите оптимальные настройки для финансового сектора.



Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	Типовые контрольные задания
	Системно подходит к выбору математических методов и информационных технологий для решения конкретных финансово-экономических задач в профессиональной области.	Знать: основы обеспечения безопасности объектов информатизации прикладного уровня в организациях КФС. Уметь: разрабатывать предложения по совершенствованию методологии обеспечения операционной надежности (киберустойчивости) в организациях КФС.	Выполните одно из заданий: • Проведите аудит внутренних регламентов организации на соответствие требованиям Положений Банка России (например, Положение ЦБ № 850-П для банков или 779-П для некредитных финансовых организаций). Выявите «узкие места» и сформируйте план по устранению регуляторных и методологических разрывов. • Опишите методику расчета сигнальных и контрольных значений допустимой доли деградации технологических процессов. Разработайте формулы и шаблоны для фиксации инцидентов операционной надежности с учетом ведения базы событий операционных рисков. • Спроектируйте сценарий реагирования на масштабную кибератаку (например, вирус-шифровальщик или DDoS-атака). Установите целевое время восстановления и допустимую потерю данных для критически важных технологических процессов организации. • Сформируйте регламент проведения регулярного тестирования объектов информационной инфраструктуры. Определите периодичность и методы валидации (анализ уязвимостей, нагрузочное тестирование, киберучения/Red Teaming), требуемые стандартом ГОСТ Р 57580.1-2017



Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	Типовые контрольные задания
	Анализирует результаты исследования математических моделей финансово-экономических задач и делает на их основании количественные и качественные выводы и рекомендации по принятию финансово-экономических решений.	Знать: Специфика платежных процессов в организациях КФС Уметь: Применять организационные и технические меры обеспечения операционной надежности (киберустойчивости) в организациях КФС	Выполните одно из заданий: 1. Определение критических процессов: • Составьте перечень (реестр) из 3–5 критически важных технологических процессов вашей организации (например, проведение платежей, выдача кредита, оформление полиса). • Определите объекты информационной инфраструктуры (серверы, базы данных, ПО), которые обеспечивают работу каждого процесса. 2. Установление показателей операционной надежности. Установите пороговые значения допустимого времени простоя и деградации процессов согласно требованиям регулятора (например, недопустимость простоя процесса более чем на 2 часа). • Рассчитайте целевые показатели надежности, такие как коэффициент готовности 3. Организационные и технические меры. Опишите комплекс мер для поддержания непрерывности: • Организационные: регламент распределения зон ответственности между ИТ и ИБ, разработка плана действий в случае инцидентов. • Технические: резервное копирование критических данных, дублирование каналов связи, защита от вредоносного ПО и DDoS-атак, контроль доступа.



Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	Типовые контрольные задания
ПKN-4. Способность оценивать показатели деятельности экономических субъектов	Проводит анализ внешней и внутренней среды ведения бизнеса, выявляет основные факторы экономического роста, оценивает эффективность формирования и использования производственного потенциала экономических субъектов.	Знать: угрозы безопасности информации, в том числе безопасности персональных данных, в автоматизированных системах в организациях КФС. Уметь: планировать и организовывать контроль выполнения организационных технических мер по защите информации, в том числе по защите персональных данных, в организациях КФС.	Задание 1: опишите реализацию базового набора организационных и технических мер: • Физическая безопасность: организация контроля доступа в помещения, где хранятся носители данных или установлены серверы. • Техническая защита: применение сертифицированных средств защиты информации, межсетевых экранов, антивирусов и средств криптографической защиты. • Организационные меры: утверждение локальных нормативных актов (политика ИБ, инструкции пользователей), обучение и ознакомление сотрудников с правилами работы с ПДн под роспись. Задание 2: опишите, как будет осуществляться периодический мониторинг: • Аудит и оценка соответствия: проведение регулярных проверок (не реже 1-2 раз в год) эффективности внедренных мер защиты, включая привлечение сторонних лицензиатов ФСТЭК/ФСБ. • Контроль инцидентов: регистрация событий, связанных с защитой информации, и порядок реагирования на утечки. • Контроль доступа: регулярная ревизия прав доступа сотрудников к критическим базам данных (увольнение, перевод).



Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	Типовые контрольные задания
	Рассчитывает и интерпретирует показатели деятельности экономических субъектов.	Знать: принципы целеполагания, виды и методы организационного планирования. Уметь: устанавливать и поддерживать деловые контакты, связи, отношения с сотрудниками и заинтересованными сторонами по вопросам управления рисками информационной безопасности, обеспечения информационной безопасности и операционной надежности (киберустойчивости) в организациях КФС.	Задание: составьте список лиц, ответственных за разные уровни защиты: • Руководство банка: принимают решения о риск-аппетите. • Бизнес-подразделения: владельцы активов, формирующие требования к доступности услуг. • IT-департамент: отвечают за операционную надежность и внедрение технических мер. • Служба ИБ и управления рисками: выявление угроз, анализ инцидентов



Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	Типовые контрольные задания
ПКП-2. Способность осуществлять мониторинг экономических, промышленных и корпоративных изменений посредством анализа информации и интерпретировать данные, связанные с финансовыми решениями, включая цены, прибыль, устойчивость,	Грамотно использует достоверные источники финансово-экономической и статистической информации для сбора, обработки и анализа данных с целью дальнейшего использования в решении экономических и финансовых задач.	Знать: законодательство Российской Федерации, нормативные правовые акты, национальные, межгосударственные и международные стандарты в области защиты информации. Уметь: планировать политику безопасности компонентов (операционных систем, баз данных, компьютерных сетей, программных систем) автоматизированной системы в организациях кредитно-финансовой сферы.	Контрольное задание: выбрать объект исследования. Вам нужно составить детальный план мероприятий для конкретного уровня защиты по ГОСТ Р 57580.1-2017 или описать требования к определенному компоненту более развернуто, уточните: • Какие именно виды финансовых операций автоматизирует ваша система? • Какой класс угроз или уровень защиты предстоит реализовать?



Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	Типовые контрольные задания
дальнейшие перспективы в плане инвестиционных рисков и экономического влияния, применяя возможности инновационных финансовых технологий	Применяет математические методы и информационные технологии проведения мониторинга экономических показателей, рассчитанных на основе данных, связанных с финансовыми решениями	Знать: правила сбора и регистрации информации об инцидентах информационной безопасности в организациях кредитно-финансовой сферы (далее по тексту - КФС). Уметь: анализировать и применять методологическую базу, требования законодательства Российской Федерации, нормативных актов Банка России, международных и национальных стандартов в области защиты информации, обеспечения инфор-	Задание: злоумышленники получили логин и пароль сотрудника, обманом заставляя его перейти по ссылке или ввести данные на поддельном сайте. Составьте отчет об инциденте поэтапно: 1. Определить тип инцидента в соответствии с перечнем, установленным нормативными актами Банка России. 2. Перечислить обязательные технические и системные артефакты, подлежащие сбору (журналы событий, IP-адреса, время входа, действия в системе). 3. Описать процесс фиксации инцидента во внутренней системе учета и контроля (IRP/SOAR) банка. 4. Составить черновик уведомления, включающий необходимый минимальный объем данных (индикаторы компрометации, время обнаружения, принятые меры).



Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	Типовые контрольные задания
		мационной безопасности, управления рисками информационной безопасности в организациях КФС, а также обнаружения, предупреждения и ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры организаций КФС, и реагирования на компьютерные инциденты.	
	Проводит оценку инвестиционных рисков и экономического	Знать: Руководящие и методические документы уполномочен-	В финансовом секторе защита информации строго регламентируется стандартами и регуляторами (Банк России, ФСТЭК, ФСБ). Ответьте на вопросы:



Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	Типовые контрольные задания
	влияния на основе полученных данных и проведенного анализа.	ных федеральных органов исполнительной власти, нормативные акты Банка России в области защиты информации, обеспечения информационной безопасности, управления рисками информационной безопасности в организациях КФС, а также в области обнаружения, предупреждения и ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной ин-	1. Какие требования должен знать специалист в области информационной безопасности применительно к КФС? 2. Как осуществляется взаимодействие с центром ГосСОПКА для предотвращения атак на критическую информационную инфраструктуру (КИИ).



Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	Типовые контрольные задания
		фраструктуры, реагирования на компьютерные инциденты Уметь: Осуществлять работу с техническими средствами защиты информации и системами, реализующими функции управления инцидентами информационной безопасности организаций КФС	



Примеры практико-ориентированных заданий

1. Контент-анализ рекламы и объявлений о приеме на работу.
2. Контент-анализ выступления, интервью или беседы в целях кибербезопасности
3. Процедуры компьютерного анализа текстов в целях кибербезопасности
4. Типичные проблемы рекомендаций в отчетах по кибербезопасности
5. Разработайте план безопасной архитектуры сети.
6. Какие типы межсетевых экранов и правила фильтрации необходимо применить для предотвращения распространения вредоносного ПО на физические исполнительные механизмы?
7. Создайте пошаговую схему безопасного обновления «железа».
8. Опишите, как использовать криптографические ключи, цифровые подписи и доверенную зону процессора. Устройство должно намертво блокировать запуск любой чужой прошивки.
9. Разработайте правила для системы обнаружения вторжений (IDS).
10. Как обнаружить аномалию в автоматизированных системах по косвенным признакам?
11. Какие ключевые российские законы и нормативные акты (например, ФЗ-187, требования ФСТЭК и ФСБ) регулируют обеспечение кибербезопасности в КФС?
12. Каковы основные требования Банка России к защите информации в финансовых организациях и как они реализуются на практике?
13. Какие международные стандарты (например, ISO/IEC 27001, NIST Cybersecurity Framework) применимы к КФС и в чем их отличие от российских требований?
14. Каковы обязанности и зоны ответственности владельцев и операторов КФС при возникновении компьютерных инцидентов согласно законодательству РФ?
15. Какова роль систем обнаружения и предотвращения вторжений (IDS/IPS) в обеспечении непрерывности работы КФС?
16. Какие методы шифрования данных (в покое и при передаче) считаются наиболее надежными для защиты финансовой информации?
17. Как обеспечивается защита конечных точек (рабочих станций, серверов) от вредоносного ПО и целевых атак в условиях КФС?
18. Каковы принципы работы и преимущества использования систем класса SIEM (Security Information and Event Management) для мониторинга событий безопасности в КФС?



Примеры вопросов для подготовки к промежуточной аттестации

1. Подготовка кадров и обеспечение доверия граждан к цифровой среде.
2. Международное сотрудничество.
3. Национальная программа «Цифровая экономика Российской Федерации».
4. Центр компетенций по обеспечению информационной безопасности и противодействию кибератакам в кредитно-финансовой сфере.
5. Надзорная деятельность.
6. Механизм построения кибербезопасности в банковской сфере.
7. Методология анализа рисков недостаточного обеспечения кибербезопасности.
8. Информационное общество и кибербезопасность.
9. Кибербезопасность в условиях развития интернета вещей и электронного банкинга.
10. Типовые атаки на организации кредитно-финансовой сферы.
11. Международный стандарт оценки защищенности ISO/IEC 27004:2009 и ГОСТ Р ИСО/МЭК 27004-2011.
12. Базовые вопросы проверки защищенности.
13. Оценка эффективности и результативности деятельности по управлению ИБ.
14. Измерение, мера измерения, показатель и метрика.
15. Метрики безопасности.
16. Системы анализа защищенности.
17. Этапы построения системы защиты информации.
18. Чем регламентируется создание политики безопасности, что включено в нее?
19. Оценка эффективности инвестиций в информационную безопасность.
20. Обеспечение компьютерной безопасности учетной информации.
21. Обеспечение информационной безопасности автоматизированных банковских систем.
22. Контур системы управления операционным риском.
23. Состав системы управления информационной безопасностью.
24. Взаимодействие с поставщиками ИТ и облачных услуг.
25. Подходы к регулированию аутсорсинга.
26. Оперативная обработка событий риска.



ПРИМЕРЫ ЭКЗАМЕНАЦИОННЫХ БИЛЕТОВ

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Информационное обеспечение деятельности органов государственной власти (15 баллов)
2. Чем регламентируется создание политики безопасности, что включено в нее? (20 баллов)
3. Оперативная обработка событий риска. Опишите алгоритм и критерии оценки. (25 баллов)

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 2

1. Взаимодействие с поставщиками ИТ и облачных услуг. (15 баллов)
2. Механизм построения кибербезопасности в банковской сфере. (20 баллов)
3. Международный стандарт оценки защищенности ISO/IEC 27004:2009 и ГОСТ Р ИСО/МЭК 27004-2011? (25 баллов)



8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Основная литература:

1. Внуков, Андрей Анатольевич Защита информации в банковских системах : учебник для вузов / А. А. Внуков. 2-е изд., испр. и доп Электрон. дан. Москва : Юрайт, 2026 246 с (Высшее образование) URL: <https://urait.ru/bcode/584051> (дата обращения: 27.02.2026). Режим доступа: Электронно-библиотечная система Юрайт, для авториз. пользователей <https://urait.ru/bcode/584051> ISBN 978-5-534-01679-6 : 1099.00. [БИК ID: RU2fURAIT2f584051]
2. Щеглов, Андрей Юрьевич Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. Электрон. дан. Москва : Юрайт, 2026 349 с (Высшее образование) URL: <https://urait.ru/bcode/583858> (дата обращения: 27.02.2026). Режим доступа: Электронно-библиотечная система Юрайт, для авториз. пользователей <https://urait.ru/bcode/583858> ISBN 978-5-534-19762-4 : 1849.00. [БИК ID: RU2fURAIT2f583858]
3. Зенков, Андрей Вячеславович Информационная безопасность и защита информации : учебник для вузов / А. В. Зенков. 2-е изд., пер. и доп Электрон. дан. Москва : Юрайт, 2026 107 с (Высшее образование) URL: <https://urait.ru/bcode/588741> (дата обращения: 27.02.2026). Режим доступа: Электронно-библиотечная система Юрайт, для авториз. пользователей <https://urait.ru/bcode/588741> ISBN 978-5-534-16388-9 : 499.00. [БИК ID: RU2fURAIT2f588741]

Дополнительная литература:

1. Крылов, Г.О. Базовые понятия информационной безопасности : Учебное пособие / Г.О. Крылов, С.Л. Ларионова, В.Л. Никитина Электрон. дан. Москва : Русайнс, 2025 257 с. Режим доступа: book.ru Internet access <https://book.ru/book/958467> ISBN 978-5-466-09255-4. [БИК ID: RU\bookru\bibl\958467]
2. Шаньгин, Владимир Федорович Комплексная защита информации в корпоративных системах : Учебное пособие / Московский институт электронной техники 1 Москва : Издательский Дом "ФОРУМ", 2022 592 с. (Высшее образование: Бакалавриат) ВО - Бакалавриат <https://znanium.com/catalog/document?id=389857> ISBN 978-5-8199-0730-6 ISBN 978-5-16-106148-0 (электр. издание) ISBN 978-5-16-013495-6 (ISBN соиздателя) . [БИК ID: RU\infra-m\znanium\bibl\1843022]



Нормативные правовые акты:

1. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 г. №149-(с изм. и доп., вступ. в силу с 31.07.2023).
2. Стратегия национальной безопасности Российской Федерации (Утверждена Указом Президента Российской Федерации от 2 июля 2021 г. № 400).
3. Доктрина информационной безопасности Российской Федерации. Указ Президента РФ от 05.12.2016 г. № 646.
4. Закон «О государственной тайне» от 21.06.1993 г. № 5485-1 (с изменениями и дополнениями).
5. Федеральный закон «О персональных данных» от 27 июля 2006 года № 152-ФЗ.
6. Положение Банка России от 08.04.2020 № 716-П "О требованиях к системе управления операционным риском в кредитной организации и банковской группе"
7. РД 50-34.698-9 Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов.

9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. Электронная библиотека Финансового университета (ЭБ) <http://elib.fa.ru/>
(<http://library.fa.ru/files/elibfa.pdf>)
2. Электронно-библиотечная система BOOK.RU <http://www.book.ru>
3. Научная электронная библиотека eLibrary.ru <http://elibrary.ru>
4. Образовательная платформа "ЮРАЙТ" <https://urait.ru/>
5. <https://www.planetaexcel.ru/>
6. Электронно-библиотечная система "Университетская библиотека ОНЛАЙН" <http://biblioclub.ru/>
7. Электронно-библиотечная система Znanium <http://www.znanium.com>
8. "Деловая онлайн библиотека" издательства "Альпина Паблишер" <http://lib.alpinadigital.ru/en/library>
9. Электронно-библиотечная система издательства "Лань" <https://e.lanbook.com/>
10. Информационно-образовательный портал Финуниверситета: <https://org.fa.ru>
11. • Электронная библиотека Финансового университета (ЭБ) <http://elib.fa.ru/>
12. • Электронно-библиотечная система BOOK.RU <http://www.book.ru>
13. • Электронно-библиотечная система «Университетская библиотека ОНЛАЙН» <http://biblioclub.ru/>



10. Методические указания для обучающихся по освоению дисциплины

Самостоятельная работа студентов реализуется в соответствии с приказом Финансового университета от 11.05.2021 № 1040/о «Об утверждении Методических рекомендаций по планированию и организации внеаудиторной самостоятельной работы студентов по образовательным программам бакалавриата и магистратуры в Финансовом университете». Промежуточная аттестация проводится в соответствии с приказом Финансового университета от 01.10.2024 № 2187/о «Об утверждении Положения о проведении текущего контроля успеваемости и промежуточной аттестации студентов, обучающихся по образовательным программам высшего образования в Финансовом университете». Кафедрой могут разрабатываться дополнительные методические рекомендации для отдельных форм проведения аудиторных занятий и самостоятельной работы студентов.



11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень необходимого программного обеспечения и информационных справочных систем

Комплект лицензионного программного обеспечения:

1. Kaspersky
2. Astra Linux

Современные профессиональные базы данных и информационные справочные системы

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

Сертифицированные программные и аппаратные средства защиты информации

1. не предусмотрены

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

1. Учебная аудитория для проведения учебных занятий, предусмотренных программой, в том числе групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенная оборудованием и техническими средствами обучения: мебель аудиторная (столы, стулья, доска аудиторная), набор демонстрационного оборудования (проектор, экран)
2. **Компьютерный класс** для проведения учебных занятий, предусмотренных программой, в том числе групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенный оборудованием и техническими средствами обучения: мебель аудиторная (столы, стулья, доска аудиторная), персональные компьютеры, набор демонстрационного оборудования (проектор, экран)
3. Доступ к сети Интернет для использования онлайн-ресурсов, репозиториев, документации.