

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

**Кафедра информационной безопасности**  
**Факультета информационных технологий и анализа больших данных**

**УТВЕРЖДАЮ**

Проректор по учебной  
и методической работе  
\_\_\_\_\_ Е. А. Каменева

«03» февраля 2025 г.

**А.Н. Велигура**

**«Управление информационной безопасностью»**

**Рабочая программа дисциплины**  
для студентов, обучающихся по направлению подготовки  
38.03.05 «Бизнес-информатика»,  
Образовательная программа  
«Цифровая трансформация управления бизнесом»  
Профиль: «ИТ-менеджмент в бизнесе»,  
«Технологии цифровых бизнес-моделей»

*Рекомендовано Ученым советом Факультета  
информационных технологий и анализа больших данных  
(протокол от «21» января 2025 г. № 51)*

*Одобрено на заседании Кафедры информационной безопасности  
(протокол от «05» декабря 2024 г. № 10)*

Москва, 2025

## СОДЕРЖАНИЕ

1. Наименование дисциплины .....	3
2. Перечень планируемых результатов освоения образовательной программы с указанием индикаторов их достижения, соотнесенных с планируемыми результатами обучения по дисциплине .....	3
3. Место дисциплины в структуре образовательной программы .....	4
4. Объем дисциплины(модуля) в зачетных единицах и в академических часах с выделением объема аудиторной (лекции, семинары) и самостоятельной работы обучающихся .....	5
5. Содержание дисциплины, структурированное по темам (разделам) дисциплины с указанием их объемов (в академических часах) и видов учебных занятий .....	5
5.1. Содержание дисциплины .....	5
5.2. Учебно-тематический план .....	8
5.3. Содержание семинаров, практических занятий .....	9
6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине .....	10
6.1. Перечень вопросов, отводимых на самостоятельное освоение дисциплины, формы внеаудиторной самостоятельной работы .....	10
6.2. Перечень вопросов, заданий, тем для подготовки к текущему контролю .....	11
7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине .....	12
8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины .....	17
9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины .....	17
10. Методические указания для обучающихся по освоению дисциплины .....	21
11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень необходимого программного обеспечения и информационных справочных систем .....	21
12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине .....	22

## 1. Наименование дисциплины

Управление информационной безопасностью

## 2. Перечень планируемых результатов освоения образовательной программы с указанием индикаторов их достижения, соотнесенных с планируемыми результатами обучения по дисциплине

Таблица 1

Код компетенции	Наименование компетенции	Индикаторы достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции
<b>УК-7</b>	Способность создавать и поддерживать безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, владеть основными методами защиты от возможных последствий аварий, катастроф, стихийных бедствий и военных конфликтов	1.Выявляет и устраняет проблемы, связанные с нарушениями техники безопасности на рабочем месте, обеспечивая безопасные условия труда.	<b>Знать</b> основные требования к технике безопасности на рабочем месте, безопасным условиям труда. <b>Уметь</b> выявлять и устранять проблемы, связанные с нарушениями техники безопасности на рабочем месте, обеспечивая безопасные условия труда
		2. Осуществляет выполнение мероприятий по защите населения и территорий в чрезвычайных ситуациях и военных конфликтах.	<b>Знать</b> основные мероприятия по защите населения и территорий в чрезвычайных ситуациях и военных конфликтах. <b>Уметь</b> проводить мероприятия по защите населения и территорий в чрезвычайных ситуациях и военных конфликтах.
		3. Находит пути решения ситуаций, связанных с безопасностью жизнедеятельности людей для сохранения природной среды, обеспечения устойчивого развития общества.	<b>Знать</b> основные проблемные ситуации, связанные с безопасностью жизнедеятельности людей, сохранением природной среды, обеспечением устойчивого развития общества. <b>Уметь</b> находить пути решения ситуаций, связанных с безопасностью жизнедеятельности людей для сохранения природной

			среды, обеспечения устойчивого развития общества.
		4. Действует в экстремальных и чрезвычайных ситуациях, применяя на практике основные способы выживания	<b>Знать</b> основные способы выживания в экстремальных и чрезвычайных ситуациях. <b>Уметь</b> применять на практике основные способы выживания.
<b>ПKN-12</b>	Способность применять вычислительное оборудование, системы хранения данных и инфраструктурные решения центров обработки данных	1. Проводит анализ рынка вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных.	<b>Знать</b> способы анализа рынка вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных. <b>Уметь</b> проводить анализ рынка вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных.
		2. Консультирует по использованию вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных.	<b>Знать</b> основные варианты использования вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных. <b>Уметь</b> формулировать предложения по использованию вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных.

### 3. Место дисциплины в структуре образовательной программы

Дисциплина «Управление информационной безопасностью» относится к общепрофессиональному циклу.

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

Таблица 2

Вид учебной работы по дисциплине	Всего (в з.е и часах)	Семестр 2 (в часах)
<b>Общая трудоемкость дисциплины</b>	3 з.е./108	108
<b>Контактная работа-Аудиторные занятия</b>	50	50
<i>Лекции</i>	16	16
<i>Семинары, практические занятия</i>	34	34
<b>Самостоятельная работа</b>	58	58
Вид текущего контроля	Контрольная работа	Контрольная работа
Вид промежуточной аттестации	Зачет	Зачет

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

##### 5.1. Содержание дисциплины

##### Раздел 1. Общие вопросы управления ИБ организации

Основные понятия, связанные с управлением ИБ Понятия: информационная безопасность, информационная безопасность объекта информатизации, безопасность информации, безопасность информационной технологии и их роль в процессах управления ИБ. Угроза (безопасности информации), уязвимость (объекта защиты), риск ИБ. Сущность управления ИБ организации. Необходимость управления обеспечением ИБ организации. Процессный подход к управлению ИБ. Системный подход к управлению ИБ. Управление обеспечением ИБ организации как процесс. Циклическая модель PDCA применительно к управлению ИБ. Роль стандартов в управлении ИБ. Основные организации, издающие стандарты по вопросам управления ИБ. Международная организация по стандартизации (ИСО, ISO). Международная электротехническая комиссия (МЭК, IEC). Национальные органы по стандартизации: Федеральное агентство по техническому регулированию и метрологии (Росстандарт), Британский институт стандартов (BSI), Национальный институт стандартов и технологий США (NIST), Федеральное ведомство по безопасности информационных технологий (BSI, Германия). Общие сведения о стандартах США, Великобритании и Германии, касающихся вопросов управления ИБ. Комплекс стандартов и рекомендаций

Банка России по управлению ИБ. Общие требования к системам менеджмента ИБ. Нормы и правила менеджмента ИБ. Цели и меры управления. Организация обеспечения информационной безопасности. Области контроля. Международные стандарты по общим вопросам управления ИБ (ISO 27001, ISO 27002, ISO 27003) и гармонизированные с ними российские национальные стандарты.

## Раздел 2. Специальные вопросы управления ИБ организации

### Управление информационной безопасностью финансовых организаций.

Требования и рекомендации Банка России и других регуляторов в сфере управления ИБ финансовых организаций. Комплекс СТО БР ИББС. ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер» и вопросы его использования. ГОСТ Р 57580.3-2022 «Безопасность финансовых (банковских) операций. Управление риском реализации информационных угроз и обеспечение операционной надежности» и вопросы его использования. ГОСТ Р 57580.3-2022 «Безопасность финансовых (банковских) операций. Обеспечение операционной надежности. Базовый состав организационных и технических мер». Вопросы ИБ индустрии платежных карт. ГОСТ Р ИСО/МЭК 15408 и «Профиль защиты прикладного программного обеспечения автоматизированных систем и приложений кредитных организаций и некредитных финансовых организаций».

### Отдельные направления управления ИБ.

Менеджмент риска информационной безопасности. Моделирование угроз. Менеджмент инцидентов информационной безопасности. Обеспечение непрерывности деятельности и восстановления после прерываний. Бесперебойность. Обеспечение ИБ на стадиях жизненного цикла автоматизированных систем.

## Раздел 3. Реализация системы управления ИБ организации.

### Планирование в управлении ИБ

Определение приоритетов организации для разработки системы управления ИБ организации. Определение области действия системы управления ИБ организации. Определение защищаемых активов информационной инфраструктуры организации, их классификация. Разработка политики системы управления ИБ организации на основе характеристик бизнеса, организации, ее размещения, активов и технологий. Определение подхода к оценке риска в организации. Анализ и оценка рисков. Определение и оценка различных

вариантов обработки рисков. Выбор целей и мер управления для обработки рисков.

Внедрение системы управления информационной безопасностью

Разработка плана обработки рисков. Реализация плана обработки рисков для достижения намеченных целей управления. Внедрение мер управления, выбранные на стадии планирования, для достижения целей управления. Определение способа измерения результативности выбранных мер управления или их групп и использования этих измерений для оценки результативности управления. Реализация программы по обучению и повышению квалификации сотрудников. Управление работой системой управления ИБ организации. Управление ресурсами системы управления ИБ организации. Внедрение процедур и других мер управления, обеспечивающих быстрое обнаружение событий ИБ и реагирование на инциденты, связанные с ИБ.

Анализ системы управления ИБ организации.

Выполнение процедуры мониторинга и анализа. Проведение регулярного анализа результативности системы управления ИБ организации. Измерение результативности мер управления для проверки соответствия требованиям ИБ. Периодический пересмотр оценки рисков, анализ остаточных рисков и установленных приемлемых уровней рисков с учётом происходящих изменений. Проведение внутренних аудитов системы управления ИБ организации. Проведение руководством организации анализа системы управления ИБ организации для ее оценки и определения направлений совершенствования. Обновление планов обеспечения ИБ с учетом результатов анализа и мониторинга.

Совершенствование системы управления ИБ организации.

Выявление возможностей улучшения системы управления ИБ организации. Выполнение необходимых корректирующих и предупреждающих действий. Передача подробной информации о действиях по улучшению системы управления ИБ организации всем заинтересованным сторонам. Обеспечение внедрения улучшений системы управления ИБ организации для достижения запланированных целей.

Раздел 4. Внутренние нормативные документы по управлению ИБ организации.

Документационное обеспечение управления информационной безопасностью организации.

Задачи и назначение документационного обеспечения управления информационной безопасностью организации. Иерархия внутренних нормативных документов по управлению информационной безопасностью организации. Требования к организации документационного обеспечения управления информационной безопасностью организации.

Политика информационной безопасности организации. Роль политики ИБ как основного внутреннего нормативного документа по ИБ. Содержание политики ИБ. Жизненный цикл политики ИБ

Другие документы по управлению ИБ.

Частные политики ИБ, их назначение и состав. Примеры областей обеспечения ИБ, управляемые частными политиками. Документы, содержащие положения ИБ, применяемые к процедурам обеспечения ИБ. Документы, содержащие свидетельства выполненной деятельности по обеспечению ИБ.

## 5.2. Учебно-тематический план

Таблица 3

№ п/п	Наименование разделов дисциплины	Трудоемкость в часах					Формы текущего контроля успеваемости
		Всего	Контактная работа* - Аудиторная работа			Самостоятельная работа	
			Общая, в т.ч.:	Лекции	Семинары, практические занятия		
1.	Общие вопросы управления ИБ организации	25	12	4	8	13	Доклады, презентации и дискуссии
2.	Специальные вопросы управления ИБ организации	26	12	4	8	14	Доклады, презентации и дискуссии



3.	Реализация системы управления ИБ организации.	30	14	4	10	16	Доклады, презентации и дискуссии
4.	Внутренние нормативные документы по управлению ИБ организации.	27	12	4	8	15	Доклады, презентации и дискуссии
	В целом по дисциплине	<b>108</b>	<b>50</b>	<b>16</b>	<b>34</b>	<b>58</b>	Согласно учебному плану. Контрольная работа
	Итого в %		46	32	68	54	

\*Объем контактной работы в очно-заочной/заочной формах обучения и индивидуальных учебных планах определяется соответствующими учебными планами. Темы, реализуемые в виде контактной работы, определяются преподавателем самостоятельно, исходя из уровня их сложности.

### 5.3. Содержание семинаров, практических занятий

Таблица 4

Наименование разделов дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях, рекомендуемые источники из разделов 8,9 (указывается раздел и порядковый номер источника)	Формы проведения занятий
Общие вопросы управления ИБ организации	Роль стандартов в управлении ИБ. Основные организации, издающие стандарты по вопросам управления ИБ. Комплекс стандартов и рекомендаций Банка России по управлению ИБ. Общие требования к системам менеджмента ИБ. Источники: 8.1-8.22; 9.1-9.23	Групповые дискуссии презентация основных подходов.  Учебное задание: сравнение подходов к управлению ИБ в ISO, России, США и Германии.
Специальные вопросы управления ИБ организации	Управление информационной безопасностью финансовых организаций. Требования и рекомендации Банка России и других регуляторов в сфере управления ИБ финансовых организаций. Комплекс СТО и РС БР ИББС. ГОСТ Р 57580.1 и 57580.2. Вопросы ИБ индустрии платежных карт. Отдельные направления менеджмента ИБ. Обеспечение	Групповые дискуссии презентация основных подходов.  Учебное задание: Исследование методики ГОСТ Р 57580.2

	непрерывности деятельности и восстановления после прерываний. Источники: 8.1-8.22; 9.1-9.23	
Реализация системы управления ИБ организации.	Планирование в управлении ИБ. Внедрение системы управления ИБ. Анализ системы управления ИБ. Совершенствование системы управления ИБ организации. Источники: 8.1-8.22; 9.1-9.23	групповые дискуссии презентация основных подходов.  Учебное задание: Исследование методики оценки модели угроз
Внутренние нормативные документы по управлению ИБ организации.	Иерархия внутренних нормативных документов по управлению информационной безопасностью. Требования к организации документационного обеспечения управления информационной безопасностью. Политика информационной безопасности организации. Другие документы по управлению ИБ. Источники: 8.1-8.22; 9.1-9.23	групповые дискуссии презентация основных подходов.  Учебное задание: Пример составления частных политик

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

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

Таблица 5

Наименование тем (разделов) дисциплины	Перечень вопросов, отводимых на самостоятельное освоение	Формы внеаудиторной самостоятельной работы
Общие вопросы управления ИБ организации	Стандарты систем менеджмента качества в управлении ИБ	- работа с учебной, научной и справочной литературой; - конспект; - подготовка сообщений по теме; - подготовка презентаций по теме; - выполнение учебного задания
Специальные вопросы управления ИБ организации	Положения ГОСТ Р 57580.1 в документах Банка России. Менеджмент инцидентов ИБ. Обеспечение непрерывности деятельности и восстановления после прерываний.	- работа с учебной, научной и справочной литературой; - конспект; - подготовка сообщений по теме; - подготовка презентаций по теме; - выполнение учебного задания

Наименование тем (разделов) дисциплины	Перечень вопросов, отводимых на самостоятельное освоение	Формы внеаудиторной самостоятельной работы
Реализация системы управления ИБ организации	<p>Определение подхода к оценке риска в организации.</p> <p>Управление ресурсами системы управления ИБ организации.</p> <p>Измерение результативности мер управления для проверки соответствия требованиям ИБ.</p>	<p>- работа с учебной, научной и справочной литературой;</p> <p>- конспект;</p> <p>- подготовка сообщений по теме;</p> <p>- подготовка презентаций по теме;</p> <p>- выполнение учебного задания</p>
Внутренние нормативные документы по управлению ИБ организации	Частные политики ИБ, их назначение и состав.	<p>- работа с учебной, научной и справочной литературой;</p> <p>- конспект;</p> <p>- подготовка сообщений по теме;</p> <p>- подготовка презентаций по теме;</p> <p>- выполнение учебного задания</p>

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

### *Примерный перечень тем контрольных работ*

1. Виды информации, подлежащей защите в РФ.
2. Оценка соответствия требованиям ИБ в КФО.
3. Профили защиты.
4. Профиль защиты прикладного программного обеспечения автоматизированных систем и приложений кредитных организаций и некредитных финансовых организаций
5. Ключевые требования к защите информации при осуществлении переводов денежных средств.
6. Методика оценки модели угроз и ее применение.
7. Ключевые субъекты НПС.

### *Примерный перечень вопросов для дискуссий*

1. Национальная платежная система, ее участники и требования к обеспечению ИБ .

2. Менеджмент инцидентов ИБ.
3. Управление в инфраструктуре открытых ключей.
4. Мошеннические операции в кредитно-финансовой сфере.
5. Аудит ИБ

***Примерный перечень тем докладов с презентациями***

1. Международные и национальные российские стандарты по информационной безопасности.
2. Международные и национальные российские стандарты по управлению информационной безопасностью.
3. Регулирование ИБ международных карточных платежных систем.
4. Требования к обеспечению ИБ в РФ.
5. Требования к обеспечению ИБ в финансовых организациях РФ.

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

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

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

Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные и индикаторами достижения компетенций	Типовые контрольные задания
УК-7 Способность создавать и поддерживать безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, владеть основными методами защиты от возможных последствий аварий, катастроф, стихийных бедствий и военных конфликтов	Индикатор 1. Выявляет и устраняет проблемы, связанные с нарушениями техники безопасности на рабочем месте, обеспечивая безопасные условия труда.	<b>Знать</b> основные требования к технике безопасности на рабочем месте, безопасным условиям труда. <b>Уметь</b> выявлять и устранять проблемы, связанные с нарушениями техники безопасности на рабочем месте, обеспечивая безопасные условия труда	Составить план контроля соблюдения техники безопасности на рабочем месте
	Индикатор 2. Осуществляет выполнение мероприятий по защите населения и территорий в чрезвычайных ситуациях и военных конфликтах.	<b>Знать</b> основные мероприятия по защите населения и территорий в чрезвычайных ситуациях и военных конфликтах. <b>Уметь</b> проводить мероприятия по защите населения и территорий в чрезвычайных ситуациях и военных конфликтах.	Составить проект мероприятий по действиям в чрезвычайных ситуациях
	Индикатор 3. Находит пути решения ситуаций, связанных с безопасностью жизнедеятельности людей для сохранения природной среды, обеспечения устойчивого развития общества.	<b>Знать</b> основные проблемные ситуации, связанные с безопасностью жизнедеятельности людей, сохранением природной среды, обеспечением устойчивого развития общества. <b>Уметь</b> находить пути решения	Составить план проведения тренировок по действиям в чрезвычайных ситуациях

Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные и индикаторами достижения компетенций	Типовые контрольные задания
		ситуаций, связанных с безопасностью жизнедеятельности людей для сохранения природной среды, обеспечения устойчивого развития общества.	
	Индикатор 4. Действует в экстремальных и чрезвычайных ситуациях, применяя на практике основные способы выживания	<b>Знать</b> основные способы выживания в экстремальных и чрезвычайных ситуациях. <b>Уметь</b> применять на практике основные способы выживания.	Составить проект методических рекомендаций по применению на практике основных способов выживания.
ПKN-12 Способность применять вычислительное оборудование, системы хранения данных и инфраструктурные решения центров обработки данных	Индикатор 1. Проводит анализ рынка вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных.	<b>Знать</b> способы анализа рынка вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных. <b>Уметь</b> проводить анализ рынка вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных.	Составить аналитический обзор инфраструктурных решений центров обработки данных.
	Индикатор 2. Консультирует по использованию вычислительного оборудования, систем хранения данных и инфраструктурных	<b>Знать</b> основные варианты использования вычислительного оборудования, систем хранения данных и инфраструктурных	Изложить варианты сегментации вычислительного оборудования центров обработки данных согласно требованиям к защите

Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенций	Типовые контрольные задания
	решений центров обработки данных.	решений центров обработки данных. <b>Уметь</b> формулировать предложения по использованию вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных.	информации финансовых организаций.

### Примеры практико-ориентированных (ситуационных) заданий

**Задача 1.** Составьте модель угроз нарушения информационной безопасности для автоматизированной банковской системы коммерческого банка.

**Задача 2.** Составьте проект перечня событий ИБ для использования при мониторинге и выявлении инцидентов ИБ.

**Задача 3.** Переформулируйте требования стандарта PCI DSS в терминах стандарта ГОСТ Р 57580.1.

**Задача 4.** В ходе проведенного службой информационной безопасности банка были выявлены учетные записи ранее уволенных сотрудников. Предложите способы недопущения таких событий при следующих проверках со стороны службы ИБ.

**Задача 5.** В корпоративной сети кредитной организации выявлено автоматизированное рабочее место, на котором не установлен антивирус. Опишите возможные риски информационной безопасности, которые могут возникнуть.

**Задача 6.** Составьте развернутый план частной политики менеджмента инцидентов ИБ.

### Примерный перечень теоретических вопросов для подготовки к зачету

1. Какие действия и процессы составляют стадию проверки СМИБ?

2. В чем состоит обеспечение информационной безопасности автоматизированных систем на стадии разработки технических заданий?

3. Что такое информационная безопасность, информационная безопасность объекта информатизации, безопасность информации, безопасность информационной технологии, киберустойчивость (в финансовой сфере)?

4. В чем состоит обеспечение информационной безопасности автоматизированных систем на стадии проектирования?

5. Что такое система менеджмента организации и система менеджмента информационной безопасности организации?

6. В чем заключается процессный подход к управлению ИБ?

7. На какие категории подразделяются персональные данные?

8. Что такое банковская тайна?

9. Какие вопросы защиты информации в негосударственной сфере регулирует ФСТЭК?

10. Что такое идентификация и аутентификация?

11. Какие действия и процессы составляют стадию планирования СМИБ?

12. Что такое угроза (безопасности информации), уязвимость (объекта защиты), риск ИБ?

13. Что такое циклическая модель PDCA применительно к управлению ИБ?

14. Что включает выбор и применение финансовой организацией мер ЗИ согласно ГОСТ Р 57580.1-2017?

15. В каких случаях, согласно ГОСТ Р 57580.1-2017, возможно использование компенсирующих мер ЗИ? Какие условия при этом должны быть выполнены?

16. Что такое контур безопасности и уровень защиты информации, согласно ГОСТ Р 57580.1-2017? Кем и на основании чего устанавливается уровень ЗИ финансовой организации для конкретного контура безопасности?



17. Укажите стадии жизненного цикла автоматизированных систем. Чем обусловлены особенности обеспечения информационной безопасности автоматизированных систем на различных стадиях жизненного цикла?

18. Назовите основные нормативно-правовые документы в области управления информационной безопасностью.

19. Какие вопросы защиты информации в негосударственной сфере регулирует ФСБ?

20. Какие виды информации подлежат защите в соответствии с нормативными актами госрегуляторов?

21. Укажите типы факторов аутентификации.

22. Опишите основные угрозы аутентификации.

23. Укажите плюсы и минусы парольной аутентификации.

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

### **Нормативные акты**

1. Федеральный закон от 02.12.1990 № 395-1 «О банках и банковской деятельности».

2. Федеральный закон от 10 июля 2002 г. № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)».

3. Федеральный закон от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе».

4. Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».

5. Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации»

6. Федеральный закон от 06 октября 1997 г. N 131-ФЗ «О государственной тайне»

7. Федеральный закон от 29 июля 2004 г. N 98-ФЗ «О коммерческой тайне»

8. Приказ ФСТЭК России от 11.02.2013 N 17 «Об утверждении требований к защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

9. Приказ ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

10. Письмо Банка России от 24 мая 2005 г. №76-Т «Об организации управления операционным риском в кредитных организациях».

11. Положение Банка России от 8 апреля 2020 г. № 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе»

12. Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» СТО БР ИББС-1.0-2014.

13. ГОСТ Р ИСО/МЭК 27001-2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования

14. ГОСТ Р 57580.1 – 2017. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер.

15. ГОСТ Р 57580.2 – 2018. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия.

16. ГОСТ Р 57580.3-2022 «Безопасность финансовых (банковских) операций. Управление риском реализации информационных угроз и обеспечение операционной надежности. Общие положения»

17. ГОСТ Р 57580.4-2022 «Безопасность финансовых (банковских) операций. Обеспечение операционной надежности. Базовый состав организационных и технических мер»

18. ГОСТ Р ИСО ТО 13569-2007. Финансовые услуги. Рекомендации по информационной безопасности.

## **Рекомендуемая литература:**

### **а) основная:**

19. Гришина, Н. В. Основы информационной безопасности предприятия: учебное пособие / Н. В. Гришина. — Москва : ИНФРА-М, 2024. — 216 с. — ЭБС ZNANIUM. - URL: <https://znanium.com/catalog/product/2131865> (дата обращения : 09.12.2024). — Текст : электронный.

20. Защита информации: учебное пособие / А. П. Жук, Е. П. Жук, О. М. Лепешкин [и др.]. — 3-е изд. — Москва : РИОР : ИНФРА-М, 2024. — 400 с. — ЭБС ZNANIUM. - URL: <https://znanium.com/catalog/product/2140566> (дата обращения : 09.12.2024). - Текст : электронный.

**б) дополнительная:**

21. Милославская, Н. Г. Управление инцидентами информационной безопасности и непрерывностью бизнеса: учебное пособие для вузов / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. - 2-е изд. — Москва : Горячая линия-Телеком, 2016. — 170 с. — ЭБС ZNANIUM. - URL: <https://znanium.com/catalog/product/560782> (дата обращения : 09.12.2024). — Текст : электронный.

22. Шилов, А. К. Управление информационной безопасностью: учебное пособие / А. К. Шилов; Южный федеральный университет. - Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2018. - 120 с. — ЭБС ZNANIUM. - URL: <https://znanium.com/catalog/product/1021744> (дата обращения : 09.12.2024). — Текст : электронный.

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

1. Сайт Центрального банка Российской Федерации: [www.cbr.ru](http://www.cbr.ru).
2. Сайт Федеральной службы по техническому и экспортному контролю: [www.fstec.ru](http://www.fstec.ru).
3. Сайт Федерального агентства по техническому регулированию и метрологии: [www.gost.ru](http://www.gost.ru).
4. Электронная библиотека Финансового университета (ЭБ) <http://elib.fa.ru/>
5. Электронно-библиотечная система BOOK.RU <http://www.book.ru>
6. Электронно-библиотечная система «Университетская библиотека ОНЛАЙН» <http://biblioclub.ru/>

7. Электронно-библиотечная система Znanium <http://www.znanium.com>
8. Электронно-библиотечная система издательства «ЮРАЙТ»  
<https://urait.ru/>
9. Электронно-библиотечная система издательства Проспект  
<http://ebs.prospekt.org/books>
10. Электронно-библиотечная система издательства Лань  
<https://e.lanbook.com/>
11. Деловая онлайн-библиотека Alpina Digital <http://lib.alpinadigital.ru/>
12. Электронная библиотека Издательского дома «Гребенников»  
<https://grebennikon.ru/>
13. Научная электронная библиотека eLibrary.ru <http://elibrary.ru>
14. Национальная электронная библиотека <http://нэб.рф/>
15. Финансовая справочная система «Финансовый директор»  
<http://www.1fd.ru/>
16. СПАРК <https://spark-interfax.ru/>
17. Библиотека онлайн Лекций по Бизнесу и Маркетингу издательства Henry Stewart Talks
18. CNKI. Academic Reference <https://ar.oversea.cnki.net/>
19. CNKI. China Academic Journals Full-text Database  
<https://oversea.cnki.net/kns?dbcode=CFLQ>
20. Электронные продукты издательства Elsevier  
<http://www.sciencedirect.com>
21. Коллекция научных журналов Oxford University Press  
<https://academic.oup.com/journals/>
22. Электронные коллекции книг и журналов издательства Springer:  
<http://link.springer.com/>
23. База данных научных журналов издательства Wiley  
<https://onlinelibrary.wiley.com/>

## **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**

### **11.1. Комплект лицензионного программного обеспечения**

Windows, Microsoft Office

антивирус Kaspersky

### **11.2 Современные профессиональные базы данных и информационные справочные системы**

1. Информационно-правовая система «Гарант».
2. Информационно-правовая система «Консультант Плюс».
3. Электронная энциклопедия: <http://ru.wikipedia.org/wiki/Wiki>.
4. Система комплексного раскрытия информации «СКРИН» - <http://www.skrin.ru/>.

### **11.3 Сертифицированные программные и аппаратные средства защиты информации**

Не предусмотрены.

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

Занятия по дисциплине проводятся в аудиториях, оборудованных мультимедийными комплексами, компьютерами с выходом в Интернет.