

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ  
РОССИЙСКОЙ ФЕДЕРАЦИИ  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ  
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«ИНГУШСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**

**ФАКУЛЬТЕТ ЭКОНОМИКИ И УПРАВЛЕНИЯ**

**КАФЕДРА «ФИНАНСЫ И КРЕДИТ»**

УТВЕРЖДАЮ

Проректор по УР и КО

С.А. Льянова

«\_\_\_» \_\_\_\_\_ 2025г.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)**

**Б1.В.10 «ЦИФРОВАЯ БЕЗОПАСНОСТЬ В ФИНАНСОВЫХ СИСТЕМАХ»**

Направление подготовки – *бакалавриат*

**38.03.01 Экономика**

Профиль подготовки – **Экономика, финансы и учет в цифровой среде**

Квалификация выпускника – *бакалавр*

Форма обучения – **очная, очно-заочная**

Магас, 2025

Рабочая программа составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 38.03.01 Экономика (уровень высшего образования – бакалавриат) утвержденного приказом Министерства образования и науки Российской Федерации от «12\_»\_августа\_\_\_2020\_г. №\_954 и в рамках ОПОП Экономика профиль Финансы и кредит, утвержденной УС ИнгГУ, протокол № от июня 2025 г

Составитель рабочей программы: старший преподаватель Цороева М.И

Рабочая программа одобрена УМК кафедры «Финансы и кредит»  
протокол № 10/1 от « » 2025 года

Рабочая программа одобрена УМК факультета Экономики и управления  
протокол № от « » \_\_\_\_\_2025г.

## 1. Цели освоения дисциплины

Целями освоения учебной дисциплины «Цифровая безопасность в финансовых системах» являются формирование теоретических основ и практических навыков в области защиты информации от несанкционированного доступа, искажения, потери. Рассматриваются тенденции развития защиты информации с моделями возможных угроз, терминологией и основными понятиями теории защиты информации, а также с нормативными документами и методами защиты компьютерной информации. Проводится изучение современных методов защиты информации: криптография, стеганография.

*Для дисциплин, формирующих профессиональные компетенции:* Формируемые дисциплиной знания и умения готовят выпускника данной образовательной программы к выполнению следующих обобщенных трудовых функций (трудовых функций):

Код и наименование профессионального стандарта	Обобщенные трудовые функции	Трудовые функции	
		Наименование	Уровень (подуровень) квалификации
08.018 Специалист по управлению рисками	Разработка отдельных функциональных направлений управления рискам	Выработка мероприятий по воздействию на риск в разрезе отдельных видов и их экономическая оценка	В/01.6
		Документирование процесса управления рисками и корректировка реестров рисков в рамках отдельных бизнес-процессов и функциональных направлений	В/02.6
		Оказание методической помощи и поддержка процесса управления рисками для ответственных за риск сотрудников организации - владельцев риска	В/03.6
		Разработка методической и нормативной базы системы управления рисками и принципов управления рисками в рамках отдельных бизнес-процессов и функциональных направлений	В/04.6
08.045 Специалист в области инновационных финансовых технологий	Проведение подготовительных и административных работ по реализации проектов в области инновационных финансовых технологий	Сбор информации для проведения предварительного изучения и исследования тенденций в области инновационных финансовых технологий	A/01.6

		Выполнение подготовительных работ по реализации комплексных проектов в области инновационных финансовых технологий	A/02.6
--	--	---	--------

## 2. Место дисциплины в структуре ОПОП бакалавриата

Данная дисциплина (модуль) включена в раздел "Б1.В.10 Дисциплины (модули)" основной профессиональной образовательной программы 38.03.01 "Экономика" и относится к дисциплинам, формируемым участниками образовательных отношений. Осваивается на 3 курсе 6 семестра.

Изучение дисциплины «Цифровая безопасность в финансовых системах» основывается на сумме знаний, полученных студентами в процессе изучения базовых дисциплин (информатика и информационные технологии в профессиональной деятельности; цифровая экономика; 1С:Бухгалтерия; корпоративные финансы и цифровые платформы; юнит-экономика; цифровой маркетинг; Цифровая безопасность в финансовых системах; правовое регулирование финансов и цифровых активов). Дисциплина является основой для изучения последующих предметов: основы программирования и ИИ для финансистов; цифровое предпринимательство; финансовые инновации и FinTech; системы искусственного интеллекта; цифровизация закупок; цифровые финансовые экосистемы; электронный документооборот; цифровые финансы и технология блокчейн; программные продукты в финансах и учете; правовое регулирование финансов и цифровых активов.

## 3. Результаты освоения дисциплины (модуля) «Цифровая безопасность в финансовых системах»

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО по данному направлению:

Код компетенции	Наименование компетенции	Индикатор достижения компетенции (закрепленный за дисциплиной)	В результате освоения дисциплины обучающийся должен:
-----------------	--------------------------	---	--

<b>ПК-6</b>	Способен оценивать риски, связанные с использованием цифровых технологий в финансовом управлении и учете	<b>ПК-6.1</b> Выявляет и классифицирует риски, возникающие при использовании различных цифровых технологий в финансовом управлении и учёте	Знать классификацию рисков, возникающих при использовании различных цифровых технологий в финансовом управлении и учёте. Уметь выявлять и классифицировать риски, возникающие при использовании различных цифровых технологий в финансовом управлении и учёте.
		<b>ПК-6.2</b> Оценивает вероятность возникновения и потенциального воздействия выявленных рисков	Знать показатели оценки вероятности возникновения и потенциального воздействия выявленных рисков. Уметь оценивать вероятность возникновения и потенциального воздействия выявленных рисков. Владеет навыками оценки вероятности возникновения и потенциального воздействия выявленных рисков.
		<b>ПК-6.3</b> Разрабатывает и обосновывает меры по снижению и контролю рисков, связанных с использованием цифровых технологий в финансовом управлении и учёте	Знать меры по снижению и контролю рисков, связанных с использованием цифровых технологий в финансовом управлении и учёте. Уметь разрабатывать и обосновывать меры по снижению и контролю рисков, связанных с использованием цифровых технологий в финансовом управлении и учёте. Владеть мерами по снижению и контролю рисков, связанных с использованием цифровых технологий в финансовом управлении и учёте.
<b>ПК-7</b>	Способен использовать знание основных методов искусственного интеллекта в последующей профессиональной деятельности в качестве научных сотрудников, преподавателей образовательных организаций высшего образования, инженеров, технологов	<b>ПК-7.1</b> знает основные платформы ИИ;	Знать: основные принципы, теорию и практику защиты информации в банковских системах в кредитно-финансовой сфере; Уметь: производить анализ рисков информационной безопасности, контролировать эффективность мер комплексной защиты информации объектов, в том числе автоматизированных систем; Владеть: анализом рисков информационной безопасности, контролировать эффективность мер комплексной защиты информации объектов, в том числе автоматизированных систем.
		<b>ПК-7.2</b> способен использовать знания методов ИИ в профессиональной деятельности	Знать: основные принципы аппаратного, программного и информационного построения и защиты информационных банковских систем; нормативно-правовую базу в области защиты информации в банковских системах и в кредитно-финансовой сфере. Уметь: пользоваться полиграфическими и голографическими методами защиты от фальсификации документов и ценных бумаг, программным обеспечением для контроля подлинности документов; применять криптографические технологии

			<p>защиты информации, электронную цифровую подпись; проводить оценку соответствия информационной банковской системы требованиям нормативных документов и стандартам по информационной безопасности</p> <p>Владеть: пользоваться полиграфическими и голографическими методами защиты от фальсификации документов и ценных бумаг, программным обеспечением для контроля подлинности документов; применять криптографические технологии защиты информации, электронную цифровую подпись; проводить оценку соответствия информационной банковской системы требованиям нормативных документов и стандартам по информационной безопасности</p>
--	--	--	--

Общая трудоемкость дисциплины составляет 4 зачетные единицы, 144 часа.

№ п/п	Наименование разделов и тем дисциплины (модуля)	семестр	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)								Формы текущего контроля успеваемости (по неделям семестра)							
			Контактная работа					Самостоятельная работа			Форма промежуточной аттестации (по семестрам)							
			Всего	Лекции	Практические занятия	Лабораторные занятия	Др. виды контакт. работы	Всего	Курсовая работа(проект)	Подготовка к экзамену	Другие виды самостоятельной работы	Собеседование	Коллоквиум	Проверка тестов	Проверка контрол. работ	Проверка реферата	Проверка эссе и иных творческих работ	курсовая работа (проект) др.
1.	Актуальность информационной безопасности мет и метод защиты информации.	5	6	3	3			5				+				+		
2.	Методы и средства защиты информации.	5	6	3	3			5										
3.	Защита документооборота в вычислительных системах.	5	6	3	3			5										
4.	Компьютерные вирусы и механизмы борьбы с ними.	5	6	3	3			6										
5.	Международные и отечественные стандарты информационной безопасности.	5	6	3	3			6										
6.	Комплексные системы защиты информации. Алгоритмы Data Mining для задач анализа данных	5	6	3	3			6										
7.	Информационные технологии внешних взаимодействий коммерческого банка.	5	6	3	3			6										
8.	Распределение полномочий между Службой безопасности, Службой внутреннего контроля и иными подразделениями в кредитно - финансовой организации.	5	6	3	3			6				+				+		
9.	Основные способы хищения денежных средств с использованием систем удаленного управления счетом («Банк-Клиент» и «Интернет-банкинг»).	5	6	3	3			6				+			+	+		
10.	Работа с персоналом. Требования к профессиональным и моральным качествам.	5	6	3	3			6				+		+		+		
	Курсовая работа(проект)																	
	Подготовка к экзамену									27								
	Общая трудоемкость, в часах	144	60	30	30			57				Промежуточная аттестация						
												Форма						
												Зачет						
												Зачет с оценкой						

[illegible]



Общая трудоемкость дисциплины составляет 4 зачетные единицы, 144 часа.

---

---

## 4.2. Содержание дисциплины (модуля)

№ п/п	Наименование раздела дисциплины	Содержание
<i>Содержание лекционного курса</i>		
1.	Актуальность информационной безопасности мет и метод защиты информации.	Объект защиты информации. Угрозы безопасности информации в компьютерных системах.
2.	Методы и средства защиты информации.	Современные методы защиты информации. Защита от несанкционированного доступа (НСД). Ограничение, разграничение, контроль доступа, идентификация, аутентификация пользователя. СОРДИ. Таксономия нарушений информационной безопасности ВС и причины, обуславливающие их существование. Криптографические методы защиты информации. Стеганография. Концепция информационной безопасности.
3.	Защита документооборота в вычислительных системах.	Угрозы и методы защиты. Комплексный метод защиты.
4.	Компьютерные вирусы и механизмы борьбы с ними.	Источники компьютерных вирусов. Основные правила защиты. Антивирусные программы
5.	Международные и отечественные стандарты информационной безопасности.	Стандарт ISO 15408. Стандарты безопасности в Интернете, протоколы защиты передачи данных - SSL (TLS), SET, IP v. 6, IPSec. Нормативные документы, регламентирующие оценку защищенности ИТ.
6.	Комплексные системы защиты информации. Алгоритмы Data Mining для задач анализа данных	Концепция создания защищенных компьютерных систем. Этапы создания комплексной системы комплексной защиты информации
7.	Информационные технологии внешних взаимодействий коммерческого банка.	Система электронного обмена данными. Безопасность электронных банковских систем. Автоматизация банковских операций и их защита. Техника обеспечения безопасности банка.
8.	Распределение полномочий между Службой безопасности, Службой внутреннего контроля и иными подразделениями в кредитно - финансовой организации.	Классификация и характеристика основных методов защиты информации в компьютерных системах. Организационные и программно - аппаратные методы защиты. DLP-системы. Разграничение прав доступа пользователей. Идентификация и аутентификация пользователей. Системы защиты автоматизированных рабочих мест.
9.	Основные способы хищения денежных	Обеспечение безопасности электронных платежей при межбанковских расчётах. Требования к криптографической

	средств с использованием систем удаленного управления счетом («Банк-Клиент» и «Интернет-банкинг»).	системе в банковской сфере. Аутентификация электронных данных. Электронная подпись.
10.	Работа с персоналом. Требования к профессиональным и моральным качествам.	Организация приема на работу. Персонал кредитно-финансовой организации как объект защиты и как источник угрозы. Формирование модели потенциального правонарушителя, применительно к различным должностям в кредитно-финансовой организации. Создание системы персональной ответственности сотрудников кредитно-финансовых организаций

### *Темы практических/семинарских занятий*

1.	Актуальность информационной безопасности мет и метод защиты информации.	Проработка учебного материала; Подготовка к опросу; Понятия и определения в информационной безопасности. Классификация компьютерных преступлений. Работа с вопросами для самоподготовки. (Тексты лекций, контент по дисциплине, литература, методички)
2.	Методы и средства защиты информации.	Проработка учебного материала; Разработка программ по методам защиты информации: методы криптографии и стеганографии (дать описание методов, алгоритм программы, функциональные возможности метода защиты, примечания к методу, анализ криптостойкости метода защиты). Подготовка отчета. Подготовка презентации.
3.	Защита документооборота в вычислительных системах.	Проработка учебного материала; Разработка программ по методам защиты информации: методы криптографии и стеганографии (дать описание методов, алгоритм программы, функциональные возможности метода защиты, примечания к методу, анализ криптостойкости метода защиты). Подготовка отчета. Подготовка презентации
4.	Компьютерные вирусы и механизмы борьбы с ними.	Изучение основных нормативно-правовых документов в сфере защиты данных. Законодательство в банковской сфере

5.	Международные и отечественные стандарты информационной безопасности.	Изучение информационных сервисов для получения данных об организациях или гражданах для снижения репутационных и экономических рисков при ведении бизнес - процессов
6.	Комплексные системы защиты информации. Алгоритмы Data Mining для задач анализа данных	Комплексные системы защиты информации. Алгоритмы Data Mining для задач анализа данных
7.	Информационные технологии внешних взаимодействий коммерческого банка.	Разработка защищенной базы данных финансовой организации в СУБД Access.
8.	Распределение полномочий между Службой безопасности, Службой внутреннего контроля и иными подразделениями в кредитно - финансовой организации.	Изучение информационных сервисов для получения данных об организациях или гражданах для снижения репутационных и экономических рисков при ведении бизнес - процессов
9.	Основные способы хищения денежных средств с использованием систем удаленного управления счетом («Банк-Клиент» и «Интернет-банкинг»).	Таксономия нарушений информационной безопасности ВС и причины, обуславливающие их существования
10.	Работа с персоналом. Требования к профессиональным и моральным качествам.	Методы и средства защиты информации. Современные методы защиты информации. Защита от несанкционированного доступа (НСД). Ограничение, разграничение, контроль доступа, идентификация, аутентификация пользователя. СОРДИ. Таксономия нарушений информационной безопасности ВС и причины, обуславливающие их существование. Криптографические методы защиты информации. Стеганография. Концепция информационной безопасности.

## 5. Образовательные технологии

В соответствии с требованиями ФГОС ВО по направлению подготовки реализация компетентностного подхода предусматривает широкое использование в учебном процессе активных и интерактивных форм проведения занятий (компьютерных симуляций, деловых и

ролевых игр, разбор конкретных ситуаций, психологические и иные тренинги) в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся. В рамках учебных курсов предусмотрены встречи с представителями российских и зарубежных компаний, государственных и общественных организаций, мастер-классы экспертов и специалистов.

В процессе преподавания лекционный материал преподносится в интерактивной форме, в том числе с использованием средств мультимедийной техники. Обсуждение проблем, выносимых на практические занятия, происходит не столько в традиционной форме контроля текущих знаний, сколько ориентировано на творческое осмысление студентами наиболее сложных вопросов в ходе обобщения ими современной практики финансового менеджмента. Обсуждение строится в форме дискуссии, с учетом выполнения самостоятельной работы.

Для достижения поставленных целей преподавания дисциплины реализуются следующие средства, способы и организационные мероприятия:

- изучение теоретического материала дисциплины на лекциях с использованием компьютерных технологий;
- самостоятельное изучение теоретического материала дисциплины с использованием *Internet*-ресурсов, информационных баз, методических разработок, специальной учебной и научной литературы, специализированных компьютерных программ;
- закрепление теоретического материала при проведении практических работ с использованием специализированных программ, выполнения проблемно-ориентированных, поисковых, творческих заданий;
- применение тестовых методик.

*Активные и интерактивные формы проведения учебных занятий по дисциплине*

№	Семестр	Тема программы дисциплины	Применяемые технологии	Кол-во аудит. часов
2	5	Выбор объекта, вида и метода его аналитики. Разработка и демонстрация программной системы, реализующей метод интеллектуального анализа данных выбранного объекта	Разбор конкретных ситуаций. Подготовка программных систем по нескольким объектам.	4
3	5	Модификация и демонстрация разработанной программной системы для получения лингвистического резюмирования результатов анализа выбранного объекта.	Лабораторная работа	2
4	5	Изучение методов предиктивной аналитики на основе временных рядов.	Круглый стол	4
5	5	Проведение анализа данных: поиск скрытых зависимостей в данных.	Лабораторная работа	4

		Итого часов		18
--	--	-------------	--	----

**6. Учебно-методическое обеспечение самостоятельной работы студентов. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины.**

Формами проведения учебных занятий и формами заданий для самостоятельной работы обучающихся в аудитории под контролем преподавателя являются: контрольная работа; решение задач; коллоквиум; тестирование; ответы на вопросы; собеседование; индивидуальные консультации; групповые консультации; проверка правильности выполнения домашнего задания; доклад и его обсуждение; деловая игра; ролевая игра; разбор кейса (производственной ситуации); формулирование вопросов по теме; аннотирование учебного материала и т.д.

Самостоятельная работа обучающихся в компьютерном классе (в дистанционном режиме) включает следующие организационные формы учебной деятельности: работа с электронным учебником, просмотр видеолекций, работа с компьютерными тренажерами, компьютерное тестирование, изучение дополнительных тем занятий, выполнение домашних заданий и т.д.

*Внеаудиторная самостоятельная работа обучающегося* полностью осуществляется самим обучающимся. Виды внеаудиторной самостоятельной работы обучающегося: чтение текста (учебника, первоисточника, дополнительной литературы, иностранных источников); аналитическую обработку текста (аннотирование, рецензирование, реферирование, контент-анализ и др.); графическое изображение структуры текста; выписки из текста; составление плана и тезисов ответа на контрольные вопросы; составление таблиц для систематизации учебного материала; изучение карт и других материалов; работа со словарями и справочниками; составление библиографии; подготовка сообщений к выступлению на семинаре, конференции; подготовка рефератов, докладов, ознакомление с нормативными документами; учебно-исследовательская работа; использование аудио- и видеозаписей, компьютерной техники и Интернета.

Для самостоятельной работы студентам рекомендуются три вида учебно-методического обеспечения: 1) конспект лекций, 2) нормативно-правовые акты, 3) основная и дополнительная литература.

В учебном процессе используются устные и письменные формы контроля:

Устные формы контроля – Устный опрос (УО):

собеседование (УО-1),

коллоквиум (УО-2),

Письменные формы контроля – Письменные работы (ПР):

тесты (ПР-1),

контрольные работы (ПР-2),  
эссе (ПР-3),  
рефераты (ПР-4),

Таблица 6.1.

*Содержание, формы и методы контроля, показатели и критерии оценки  
самостоятельной работы для очной формы обучения*

№ п/п	Раздел дисциплины	Труд оем- кость в часах	Вид работы	Форма кон троля	Источники
1.	Актуальность информационно й безопасности мет и метод защиты информации.	5	Подготовиться к практическому занятию.	УО-1 ПР-1 ПР-4	<p>1) 1) Розанов Д.А. Основы финансовой грамотности и безопасности [Электронный ресурс]: учебно-методическое пособие/ Розанов Д.А., Прохорова Е.А.— Электрон. текстовые данные.— Армавир: Армавирский государственный педагогический университет, 2024.— 152 с.— Режим доступа: <a href="https://ipr-smart.ru/144333">https://ipr-smart.ru/144333</a>.</p> <p>2) Кузовкова, Т. А. Экономическая безопасность бизнеса в цифровой среде : учебное пособие / Т. А. Кузовкова, Т. Ю. Салютин. — Москва : Ай Пи Ар Медиа, 2023. — 128 с. — ISBN 978-5-4497-2278-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <a href="https://www.iprbookshop.ru/132156.html">https://www.iprbookshop.ru/132156.html</a></p> <p>3) Экономическая и информационная безопасность. Цифровые и автоматизированные промышленные электронные устройства. Лабораторный практикум : учебное пособие / А. Н. Брысин, Ю. А. Журавлева, С. А. Микаева, А. С. Микаева. — Москва, Вологда : Инфра-Инженерия, 2024. — 264 с. — ISBN 978-5-9729-1842-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <a href="https://www.iprbookshop.ru/143637.html">https://www.iprbookshop.ru/143637.html</a></p>
2.	Методы и средства защиты информации.	5	Подготовиться к практическому занятию.	УО-1 ПР-1 ПР-4	<p>3) Экономическая и информационная безопасность. Цифровые и автоматизированные промышленные электронные устройства. Лабораторный практикум : учебное пособие / А. Н. Брысин, Ю. А. Журавлева, С. А. Микаева, А. С. Микаева. — Москва, Вологда : Инфра-Инженерия, 2024. — 264 с. — ISBN 978-5-9729-1842-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <a href="https://www.iprbookshop.ru/143637.html">https://www.iprbookshop.ru/143637.html</a></p> <p>4) Жданова, С. Ю. Психологическая безопасность личности в информационно-цифровом пространстве : учебно-методическое пособие / С. Ю. Жданова, В. С. Краева. — Пермь : Пермский государственный национальный исследовательский университет, 2024. — 93 с. — ISBN 978-5-7944-4118-5. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL:</p>



					<p><a href="https://www.iprbookshop.ru/149615.html">https://www.iprbookshop.ru/149615.html</a></p> <p>5) Суглобов, А. Е. Экономическая безопасность предприятия : учебное пособие для студентов вузов, обучающихся по специальности «Экономическая безопасность» / А. Е. Суглобов, С. А. Хмелев, Е. А. Орлова. — Москва : ЮНИТИ-ДАНА, 2017. — 271 с. — ISBN 978-5-238-02378-6. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <a href="https://www.iprbookshop.ru/109225.html">https://www.iprbookshop.ru/109225.html</a></p>
3.	Защита документооборота в вычислительных системах.	5	Подготовиться к практическому занятию.	УО-1 ПР-1 ПР-4	<p>1) Белоус, А. И. Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения / А. И. Белоус, В. А. Солодуха. — Москва : Техносфера, 2021. — 482 с. — ISBN 978-5-94836-612-8. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <a href="https://www.iprbookshop.ru/108023.html">https://www.iprbookshop.ru/108023.html</a></p> <p>2) Велигура, А. Н. Комбинаторика и теория графов для кибербезопасности. Конспект лекций : учебное пособие / А. Н. Велигура. — Москва : Национальный исследовательский ядерный университет «МИФИ», 2021. — 200 с. — ISBN 978-5-7262-2836-5. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <a href="https://www.iprbookshop.ru/125492.html">https://www.iprbookshop.ru/125492.html</a></p>
4.	Компьютерные вирусы и механизмы борьбы с ними.	6	Подготовиться к практическому занятию.	УО-1 ПР-1 ПР-4	<p>1) Розанов Д.А. Основы финансовой грамотности и безопасности [Электронный ресурс]: учебно-методическое пособие/ Розанов Д.А., Прохорова Е.А.— Электрон. текстовые данные.— Армавир: Армавирский государственный педагогический университет, 2024.— 152 с.— Режим доступа: <a href="https://ipr-smart.ru/144333">https://ipr-smart.ru/144333</a>.</p> <p>2) Кузовкова, Т. А. Экономическая безопасность бизнеса в цифровой среде : учебное пособие / Т. А. Кузовкова, Т. Ю. Салютин. — Москва : Ай Пи Ар Медиа, 2023. — 128 с. — ISBN 978-5-4497-2278-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <a href="https://www.iprbookshop.ru/132156.html">https://www.iprbookshop.ru/132156.html</a></p> <p>3) Экономическая и информационная безопасность. Цифровые и автоматизированные промышленные электронные устройства. Лабораторный практикум : учебное пособие / А. Н. Брысин, Ю. А. Журавлева, С. А. Микаева, А. С. Микаева. — Москва, Вологда : Инфра-Инженерия, 2024. — 264 с. — ISBN 978-5-9729-1842-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <a href="https://www.iprbookshop.ru/143637.html">https://www.iprbookshop.ru/143637.html</a></p>

5.	Международные и отечественные стандарты информационно й безопасности.	6	Подготовиться практическому занятию.	к	УО-1 ПР-1 ПР-4	<p>1) Экономическая и информационная безопасность. Цифровые и автоматизированные промышленные электронные устройства. Лабораторный практикум : учебное пособие / А. Н. Брысин, Ю. А. Журавлева, С. А. Микаева, А. С. Микаева. — Москва, Вологда : Инфра-Инженерия, 2024. — 264 с. — ISBN 978-5-9729-1842-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <a href="https://www.iprbookshop.ru/143637.html">https://www.iprbookshop.ru/143637.html</a></p> <p>2) Жданова, С. Ю. Психологическая безопасность личности в информационно-цифровом пространстве : учебно-методическое пособие / С. Ю. Жданова, В. С. Краева. — Пермь : Пермский государственный национальный исследовательский университет, 2024. — 93 с. — ISBN 978-5-7944-4118-5. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <a href="https://www.iprbookshop.ru/149615.html">https://www.iprbookshop.ru/149615.html</a></p> <p>3) Суглобов, А. Е. Экономическая безопасность предприятия : учебное пособие для студентов вузов, обучающихся по специальности «Экономическая безопасность» / А. Е. Суглобов, С. А. Хмелев, Е. А. Орлова. — Москва : ЮНИТИ-ДАНА, 2017. — 271 с. — ISBN 978-5-238-02378-6. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <a href="https://www.iprbookshop.ru/109225.html">https://www.iprbookshop.ru/109225.html</a></p>
6.	Комплексные системы защиты информации.	6	Подготовиться практическому занятию.	к	УО-1 ПР-1 ПР-4	<p>1) Белоус, А. И. Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения / А. И. Белоус, В. А. Солодуха. — Москва : Техносфера, 2021. — 482 с. — ISBN 978-5-94836-612-8. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <a href="https://www.iprbookshop.ru/108023.html">https://www.iprbookshop.ru/108023.html</a></p> <p>2) Велигура, А. Н. Комбинаторика и теория графов для кибербезопасности. Конспект лекций : учебное пособие / А. Н. Велигура. — Москва : Национальный исследовательский ядерный университет «МИФИ», 2021. — 200 с. — ISBN 978-5-7262-2836-5. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <a href="https://www.iprbookshop.ru/125492.html">https://www.iprbookshop.ru/125492.html</a></p>
7.	Информационны е технологии внешних взаимодействий коммерческого банка.	6	Подготовиться практическому занятию.	к	УО-1 ПР-1 ПР-4	<p>1) Кузовкова, Т. А. Экономическая безопасность бизнеса в цифровой среде : учебное пособие / Т. А. Кузовкова, Т. Ю. Салютин. — Москва : Ай Пи Ар Медиа, 2023. — 128 с. — ISBN 978-5-4497-2278-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL:</p>

					<p><a href="https://www.iprbookshop.ru/132156.html">https://www.iprbookshop.ru/132156.html</a></p> <p>2) Экономическая и информационная безопасность. Цифровые и автоматизированные промышленные электронные устройства. Лабораторный практикум : учебное пособие / А. Н. Брысин, Ю. А. Журавлева, С. А. Микаева, А. С. Микаева. — Москва, Вологда : Инфра-Инженерия, 2024. — 264 с. — ISBN 978-5-9729-1842-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <a href="https://www.iprbookshop.ru/143637.html">https://www.iprbookshop.ru/143637.html</a></p> <p>3) Жданова, С. Ю. Психологическая безопасность личности в информационно-цифровом пространстве : учебно-методическое пособие / С. Ю. Жданова, В. С. Краева. — Пермь : Пермский государственный национальный исследовательский университет, 2024. — 93 с. — ISBN 978-5-7944-4118-5. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <a href="https://www.iprbookshop.ru/149615.html">https://www.iprbookshop.ru/149615.html</a></p>
8.	Распределение полномочий между Службой безопасности, Службой внутреннего контроля и иными подразделениям и в кредитно - финансовой организации.	6	Подготовиться к практическому занятию.	УО-1 ПР-1 ПР-4	<p>1) Розанов Д.А. Основы финансовой грамотности и безопасности [Электронный ресурс]: учебно-методическое пособие/ Розанов Д.А., Прохорова Е.А.— Электрон. текстовые данные.— Армавир: Армавирский государственный педагогический университет, 2024.— 152 с.— Режим доступа: <a href="https://ipr-smart.ru/144333">https://ipr-smart.ru/144333</a>.</p> <p>2) Кузовкова, Т. А. Экономическая безопасность бизнеса в цифровой среде : учебное пособие / Т. А. Кузовкова, Т. Ю. Салюткина. — Москва : Ай Пи Ар Медиа, 2023. — 128 с. — ISBN 978-5-4497-2278-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <a href="https://www.iprbookshop.ru/132156.html">https://www.iprbookshop.ru/132156.html</a></p> <p>3) Экономическая и информационная безопасность. Цифровые и автоматизированные промышленные электронные устройства. Лабораторный практикум : учебное пособие / А. Н. Брысин, Ю. А. Журавлева, С. А. Микаева, А. С. Микаева. — Москва, Вологда : Инфра-Инженерия, 2024. — 264 с. — ISBN 978-5-9729-1842-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <a href="https://www.iprbookshop.ru/143637.html">https://www.iprbookshop.ru/143637.html</a></p>
9.	Основные способы хищения денежных средств с использованием систем	6	Подготовиться к практическому занятию.	УО-1 ПР-1 ПР-4	<p>1) Экономическая и информационная безопасность. Цифровые и автоматизированные промышленные электронные устройства. Лабораторный практикум : учебное пособие / А. Н. Брысин, Ю. А. Журавлева, С. А. Микаева, А. С. Микаева. — Москва, Вологда : Инфра-Инженерия, 2024. — 264 с. — ISBN</p>

	удаленного управления счетом («Банк-Клиент» и «Интернет-банкинг»).				<p>978-5-9729-1842-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <a href="https://www.iprbookshop.ru/143637.html">https://www.iprbookshop.ru/143637.html</a></p> <p>2) Жданова, С. Ю. Психологическая безопасность личности в информационно-цифровом пространстве : учебно-методическое пособие / С. Ю. Жданова, В. С. Краева. — Пермь : Пермский государственный национальный исследовательский университет, 2024. — 93 с. — ISBN 978-5-7944-4118-5. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <a href="https://www.iprbookshop.ru/149615.html">https://www.iprbookshop.ru/149615.html</a></p> <p>3) Суглобов, А. Е. Экономическая безопасность предприятия : учебное пособие для студентов вузов, обучающихся по специальности «Экономическая безопасность» / А. Е. Суглобов, С. А. Хмелев, Е. А. Орлова. — Москва : ЮНИТИ-ДАНА, 2017. — 271 с. — ISBN 978-5-238-02378-6. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <a href="https://www.iprbookshop.ru/109225.html">https://www.iprbookshop.ru/109225.html</a></p>
10.	Работа с персоналом. Требования к профессиональным и моральным качествам.	6	Подготовиться к практическому занятию.	УО-1 ПР-1 ПР-4	<p>2) Кузовкова, Т. А. Экономическая безопасность бизнеса в цифровой среде : учебное пособие / Т. А. Кузовкова, Т. Ю. Салютин. — Москва : Ай Пи Ар Медиа, 2023. — 128 с. — ISBN 978-5-4497-2278-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <a href="https://www.iprbookshop.ru/132156.html">https://www.iprbookshop.ru/132156.html</a></p> <p>3) Экономическая и информационная безопасность. Цифровые и автоматизированные промышленные электронные устройства. Лабораторный практикум : учебное пособие / А. Н. Брысин, Ю. А. Журавлева, С. А. Микаева, А. С. Микаева. — Москва, Вологда : Инфра-Инженерия, 2024. — 264 с. — ISBN 978-5-9729-1842-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <a href="https://www.iprbookshop.ru/143637.html">https://www.iprbookshop.ru/143637.html</a></p> <p>4) Жданова, С. Ю. Психологическая безопасность личности в информационно-цифровом пространстве : учебно-методическое пособие / С. Ю. Жданова, В. С. Краева. — Пермь : Пермский государственный национальный исследовательский университет, 2024. — 93 с. — ISBN 978-5-7944-4118-5. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <a href="https://www.iprbookshop.ru/149615.html">https://www.iprbookshop.ru/149615.html</a></p>
	ИТОГО	49			

Фонд оценочных средств является обязательной частью рабочей программы дисциплины и представлен в Приложении 1.

## **7. Учебно-методическое и материально-техническое обеспечение дисциплины (модуля) Цифровая безопасность в финансовых системах**

### **7.1. Основная учебная литература:**

- 1) Розанов Д.А. Основы финансовой грамотности и безопасности [Электронный ресурс]: учебно-методическое пособие/ Розанов Д.А., Прохорова Е.А.— Электрон. текстовые данные.— Армавир: Армавирский государственный педагогический университет, 2024.— 152 с.— Режим доступа: <https://ipr-smart.ru/144333>.
- 2) Кузовкова, Т. А. Экономическая безопасность бизнеса в цифровой среде : учебное пособие / Т. А. Кузовкова, Т. Ю. Салютин. — Москва : Ай Пи Ар Медиа, 2023. — 128 с. — ISBN 978-5-4497-2278-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/132156.html>
- 3) Экономическая и информационная безопасность. Цифровые и автоматизированные промышленные электронные устройства. Лабораторный практикум : учебное пособие / А. Н. Брысин, Ю. А. Журавлева, С. А. Микаева, А. С. Микаева. — Москва, Вологда : Инфра-Инженерия, 2024. — 264 с. — ISBN 978-5-9729-1842-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/143637.html>
- 4) Жданова, С. Ю. Психологическая безопасность личности в информационно-цифровом пространстве : учебно-методическое пособие / С. Ю. Жданова, В. С. Краева. — Пермь : Пермский государственный национальный исследовательский университет, 2024. — 93 с. — ISBN 978-5-7944-4118-5. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/149615.html>
- 5) Суглобов, А. Е. Экономическая безопасность предприятия : учебное пособие для студентов вузов, обучающихся по специальности «Экономическая безопасность» / А. Е. Суглобов, С. А. Хмелев, Е. А. Орлова. — Москва : ЮНИТИ-ДАНА, 2017. — 271 с. — ISBN 978-5-238-02378-6. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/109225.html>

### **Дополнительная учебная литература:**

- 1) Белоус, А. И. Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения / А. И. Белоус, В. А. Солодуха. — Москва : Техносфера, 2021. — 482 с. — ISBN 978-5-94836-612-8. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/108023.html>

- 2) Велигура, А. Н. Комбинаторика и теория графов для кибербезопасности. Конспект лекций : учебное пособие / А. Н. Велигура. — Москва : Национальный исследовательский ядерный университет «МИФИ», 2021. — 200 с. — ISBN 978-5-7262-2836-5. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/125492.html>

## **7.2. Интернет-ресурсы**

- 1) Цифровой образовательный ресурс IPR SMART ([www.iprbookshop.ru](http://www.iprbookshop.ru) )
- 2) Образовательная платформа «ЮРАЙТ» <https://urait.ru/> ).
- 3) Сайт информационно-правовой системы «Гарант» - <https://www.garant.ru>

## **7.3. Программное обеспечение**

Для подготовки презентаций и их демонстрации используется программа Impress из свободного пакета офисных приложений OpenOffice.

При осуществлении образовательного процесса применяются информационные технологии, необходимые для подготовки презентационных материалов и материалов к занятиям (компьютеры с программным обеспечением для создания и показа презентаций, с доступом в сеть «Интернет», поисковые системы и справочные, профессиональные ресурсы в сети «Интернет»).

В вузе оборудованы помещения для самостоятельной работы обучающихся оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду вуза.

Программное обеспечение ОПОП: Windows 7 Professional, Microsoft Office Professional, (Государственный контракт №09 – ЗК2010 от 29.03.2010, срок действия - бессрочно) ПО «Визуальная студия тестирования», (Лицензионный договор № 7624) ПО «Приемная комиссия» (Договор № 8267) ПО «Деканат», «Планы», «Электронные ведомости» , «Система ЭИОС» Лаборатории ММИС (Лицензионный договор № 7624) ЭБС IPRbooks - № 8815/21, СПС «Гарант».

## **7.4. Материально-техническое обеспечение дисциплины**

Материально-техническое обеспечение учебного процесса определено нормативными требованиями, регламентируемыми Федеральным государственным образовательным стандартом высшего образования по направлению подготовки.

Для проведения всех видов учебных занятий и обеспечения интерактивных методов обучения, имеются столы, стулья (на группу по количеству посадочных мест с возможностью расстановки для круглых столов, дискуссий, прочее); доска интерактивная с рабочим местом

(мультимедийный проектор с экраном и рабочим местом); с доступом в информационно-коммуникационную сеть «Интернет».

В соответствии с требованиями ФГОС ВО, ОПОП ВО учтены образовательные потребности обучающихся с ограниченными возможностями здоровья, обеспечивающие условия для их эффективной реализации, а также возможности беспрепятственного доступа обучающихся с ограниченными возможностями здоровья к объектам инфраструктуры образовательного учреждения.

Реализация ОПОП обеспечена следующим м/т оснащением в части дисциплины «Цифровая безопасность в финансовых системах»:

- учебная аудитория для лекционных занятий (№ 224) 3886001,РИ, г. Магас, пр. Зязикова, 7: Стол для преподавателя - 1 шт. (состоит из 2-х секций); стул для преподавателя -1 шт.; доска - 1 шт.; трибуна-1 шт.; стол - 42 шт.; скамья-84 шт.; интерактивная доска – 1 шт. , проектор – 1 шт.: модель VIEWSONIC PJD5153 (VS15872), 2 встроенных динамика; пульт ДУ; компьютер, подключенный к кабельной сети Интернет, доступ к беспроводной сети 802.11n. 300/1000 МБ; учебно-наглядные пособия, коллекция демонстрационных плакатов, макетов, раздаточный материал;

- учебная аудитория для семинарских занятий (№223) 3886001,РИ, г. Магас, пр. Зязикова, 7: Стол для преподавателя - 1 шт. (состоит из 2-х секций); стул для преподавателя -1 шт.; доска - 1 шт.; переносной ноутбук ASUS - 1 шт.; проектор – 1 шт.: модель VIEWSONIC PJD5153 (VS15872). экран на треноге; стол - 22 шт.; стулья-44 шт.;

- помещения для самостоятельной работы: № 236: Компьютеры – 17 шт., подключенные к сети Интернет, библиотека, учебно-методические материалы, наглядные иллюстрированные таблицы и схемы.

**Сведения о переутверждении программы на очередной учебный год и регистрации изменений**

Учебный год	Решение кафедры (№ протокола, дата)	Внесенные изменения	Подпись зав. кафедрой



## Фонд оценочных средств

## 1. Шкала оценивания, показатели и критерии оценивания образовательных результатов обучающегося во время текущей аттестации

Шкала оценивания	Показатели и критерии оценивания
5, «отлично»	Оценка «отлично» ставится, если студент строит ответ логично в соответствии с планом, показывает максимально глубокие знания профессиональных терминов, понятий, категорий, концепций и теорий. Устанавливает содержательные межпредметные связи. Развернуто аргументирует выдвигаемые положения, приводит убедительные примеры.
4, «хорошо»	Оценка «хорошо» ставится, если студент строит свой ответ в соответствии с планом. В ответе представлены различные подходы к проблеме, но их обоснование недостаточно полно. Устанавливает содержательные межпредметные связи. Развернуто аргументирует выдвигаемые положения, приводит необходимые примеры, однако показывает некоторую непоследовательность анализа. Выводы правильны. Речь грамотна, используется профессиональная лексика.
3, «удовлетворительно»	Оценка «удовлетворительно» ставится, если ответ недостаточно логически выстроен, план ответа соблюдается непоследовательно. Студент обнаруживает слабость в развернутом раскрытии профессиональных понятий. Выдвигаемые положения декларируются, но недостаточно аргументированы. Ответ носит преимущественно теоретический характер, примеры ограничены, либо отсутствуют.
2, «неудовлетворительно»	Оценка «неудовлетворительно» ставится при условии недостаточного раскрытия профессиональных понятий, категорий, концепций, теорий. Студент проявляет стремление подменить научное обоснование проблем рассуждениями обыденно-повседневного бытового характера. Ответ содержит ряд серьезных неточностей. Выводы поверхностны

## 2. Шкала оценивания, показатели и критерии оценивания образовательных результатов обучающегося во время промежуточной аттестации

Оценка экзамена (нормативная)	Показатели и критерии оценивания образовательных результатов
<i>гр.1</i>	<i>гр.2</i>
5 (отлично)	<p><b>Оценка «5 (отлично)»</b> выставляется обучающемуся, если он глубоко и прочно усвоил программный материал и демонстрирует это на занятиях и экзамене, исчерпывающе, последовательно, четко и логически стройно излагал его, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний. Причем обучающийся не затруднялся с ответом при видоизменении предложенных ему заданий, использовал в ответе материал учебной и монографической литературы, в том числе из дополнительного списка, правильно обосновывал принятое решение.</p> <p><b>Учебные достижения</b> в семестровый период и результаты рубежного контроля демонстрировали <b>высокую степень овладения программным материалом.</b></p> <p><b>Рейтинговые баллы</b> назначаются обучающемуся с учётом баллов</p>

Оценка экзамена (нормативная)	Показатели и критерии оценивания образовательных результатов
<i>гр.1</i>	<i>гр.2</i>
	текущей (на занятиях) и промежуточной (экзамен) аттестации. <b>Компетенции</b> , закреплённые за дисциплиной, <b>сформированы на уровне – высокий.</b>
4 (хорошо)	<b>Оценка «4, (хорошо)»</b> выставляется обучающемуся, если он твёрдо знает материал, грамотно и по существу излагает его на занятиях и экзамене, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приёмами их выполнения. <b>Учебные достижения</b> в семестровый период и результаты рубежного контроля демонстрируют <b>хорошую степень овладения программным материалом.</b> <b>Рейтинговые баллы</b> назначаются обучающемуся с учётом баллов текущей (на занятиях) и промежуточной (экзамен) аттестации. <b>Компетенции</b> , закреплённые за дисциплиной, <b>сформированы на уровне – хороший (средний).</b>
3 (удовлетворительно)	<b>Оценка «3 (удовлетворительно)»</b> выставляется обучающемуся, если он имеет и демонстрирует знания на занятиях и экзамене только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ. <b>Учебные достижения</b> в семестровый период и результаты рубежного контроля демонстрируют <b>достаточную (удовлетворительную) степень овладения программным материалом.</b> <b>Рейтинговые баллы</b> назначаются обучающемуся с учётом баллов текущей (на занятиях) и промежуточной (экзамен) аттестации. <b>Компетенции</b> , закреплённые за дисциплиной, <b>сформированы на уровне – достаточный.</b>
2 (не удовлетворительно)	<b>Оценка «2 (неудовлетворительно)»</b> выставляется обучающемуся, который не знает большей части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы на занятиях и экзамене. Как правило, оценка «неудовлетворительно» ставится обучающимся, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине. <b>Учебные достижения</b> в семестровый период и результаты рубежного контроля демонстрируют <b>невысокую (недостаточную) степень овладения программным материалом.</b> <b>Рейтинговые баллы</b> назначаются обучающимся с учётом баллов текущей (на занятиях) и промежуточной (экзамен) аттестации. <b>Компетенции</b> , закреплённые за дисциплиной, <b>не сформированы.</b>

**3. Типовые контрольные задания или иные материалы, необходимые для оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций**

Для оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций используются следующие типовые контрольные задания:

### **3.1. Текущий контроль успеваемости**

#### **Вопросы текущего контроля успеваемости на семинарах (практических занятиях)**

1. Основные понятия, термины и определения в области защиты информации
2. Актуальность проблемы защиты информации. Виды угроз и рисков информационной безопасности.
3. Законодательная и нормативная база правового регулирования вопросов защиты информации.
4. Требования к организации защиты конфиденциальной информации и персональных данных на предприятии.
5. Политика безопасности и формирование организационной структуры системы защиты информации на предприятии
6. Меры и средства защиты информации
7. Применения криптографических методов защиты информации при работе в сетях.
8. Аудит информационной безопасности.
9. Манипулирование людьми с целью совершения ими определенных действий или разглашения конфиденциальной информации
10. Каков косвенный ущерб от утечек информации?
- 11 Назовите методы аутентификации
- 12 В каком случае при трудоустройстве новый сотрудник, должен подписать обязательство о неразглашении служебной и коммерческой тайны
- 13 Перечислите грифы конфиденциальности документов, содержащих коммерческую или служебную тайну, в порядке их важности и обстоятельства их использования
- 14 Какие виды угроз могут возникать в сфере финансовой и банковской деятельности, требующие обеспечения безопасности?
- 15 Какие последствия может иметь нарушение безопасности в финансовой и банковской сфере для клиентов и организаций?
- 16 Какие требования предъявляются к хранению и обработке финансовых данных в соответствии с законодательством о защите персональных данных?
- 17 Какие последствия могут возникнуть при утечке финансовой информации и как их предотвратить?

- 18 Какие методы шифрования используются для защиты финансовых данных в банковской сфере?
- 19 Какие внутренние процедуры помогают обеспечить безопасность финансовых операций и данных?
- 20 Какие действия следует предпринять в случае возникновения инцидента безопасности, такого как утечка конфиденциальных данных или хищение финансовых средств?
- 21 Какие требования накладываются на финансовые учреждения в области защиты персональных данных клиентов и какие последствия могут возникнуть при нарушении этих требований?
- 22 Какое значение имеет аудит безопасности и какие методы используются для проверки систем безопасности в финансовых и банковских учреждениях?
- 23 Какая роль играет социальная инженерия при атаках на финансовые учреждения и как различные методы защиты могут помочь предотвратить такие атаки?
- 24 Что относится к организационно-управленческой информации, которая входит в состав коммерческой тайны?
- 25 Какая концепция предполагает возможность использования службой безопасности всего комплекса легитимных методов профилактики и отражения потенциальных угроз?
- 26 Какие функции реализует механизм электронной цифровой подписи?
- 27 Что такое промышленный шпионаж?
- 28 Каковы задачи обеспечения безопасности БИС в локальных или глобальных вычислительных сетях?

## **ПРИМЕРНАЯ ТЕМАТИКА РЕФЕРАТОВ**

1. Меры защиты информации: законодательного, административного, процедурного, программно-технического уровней.
2. Законодательство РФ в области информационной безопасности.
3. Информационная безопасность объекта при осуществлении международного сотрудничества. Виды угроз информационной безопасности.
4. Угрозы конституционным правам и свободам гражданина в области информационной деятельности.
5. Угрозы информационному обеспечению государственной политики Российской

Федерации.

Творческое задание (с элементами эссе)

Напишите эссе по теме:

1. Угрозы безопасности информационных и телекоммуникационных средств и систем.
2. Внешние и внутренние источники угроз информационной безопасности.
3. История развития поисковых систем.
4. Проблема общественного прогресса в истории информатики.

### Типовые тесты

1) Какая из приведенных техник является самой важной при выборе защитных мер?

- A) Анализ затрат / выгоды
- B) Результаты ALE (ALE — annual loss expectancy, ожидаемые годовые потери, т.е. «стоимость» всех инцидентов за год.)
- C) Выявление уязвимостей и угроз, являющихся причиной риска
- D) Анализ рисков

2) Что или кто определяет состав информации в перечне конфиденциальных документов фирмы:

- a. Руководитель организации, где обрабатывается информация
- b. Закон
- c. Конкретные сотрудники, к которым попадает информация для обработки

3) Сопоставьте определение канала утечки его описанию

A. позволяющие перехватывать или копировать сведения, отражающиеся в визуальной форме, это документы, информация,

выведенная на экран монитора компьютера

B. позволяющие перехватывать ведущиеся в помещении переговоры или разговоры по телефонам

C. позволяющие получать данные, выраженные в виде излучения электромагнитных волн, их дешифровка может также дать необходимые сведения

D. связанные с анализом предметов, документов и отходов, возникших в результате деятельности компании

1. акустические
2. визуально-оптические

3. электромагнитные

4. материальные

4) Какой принцип при разработке СЗИ заключается в создании нескольких последовательных рубежей защиты таким

образом, чтобы наиболее важная зона безопасности находилась внутри других зон?

А. Принцип эшелонирования обороны

В. Принцип системности

С. Принципы равнопрочности и равномощности рубежей защиты

5) Какая информация относится к общедоступной?

А. нормативные правовые акты, затрагивающие права, свободы и обязанности человека и гражданина

В. информации о состоянии окружающей среды

С. сведения из учредительных документов

Д. сведения о задержках зарплаты

6. Создание таблиц в текстовом процессоре MS Word возможно в режиме:

☐ обычном

☐ разметки

☐ структуры

☐ Web-документа

☐ схемы документа

7. Создание реквизитных элементов оформления печатных страниц в текстовом процессоре MS Word возможно в режиме:

☐ обычном

☐ разметки

☐ структуры

☐ Web-документа

☐ схемы документа

8. К базовым приемам работы с текстами в текстовом процессоре MS Word относятся:

☐ создание, сохранение и печать документа

☐ отправка документа по электронной почте

☐ ввод и редактирование текста

☐ рецензирование текста

☐ форматирование текста

9. К специальным средствам ввода текста в текстовом процессоре MS Word

относятся:

- ☐ средства отмены и возврата действий
- ☐ расширенный буфер обмена
- ☐ автотекст
- ☐ автосуммирование
- ☐ автозамена

10. К специальным средствам редактирования текста в текстовом процессоре MS Word относятся:

- ☐ режим вставки символов
- ☐ режим замены символов
- ☐ рецензирование
- ☐ тезаурус
- ☐ автоматизация проверки правописания

11. В документ MS Word можно вставить:

- ☐ формулы
- ☐ программы
- ☐ таблицы
- ☐ диаграммы
- ☐ рисунки

12. Новый макрос можно создать следующими способами:

- ☐ автоматически записать последовательность действий
- ☐ вручную написать соответствующую программу на языке VBA
- ☐ импортировать из другого файла существующий макрос
- ☐ импортировать из другого файла существующий макрос и изменить его
- ☐ изменить в уже созданный макрос и сохранить под другим именем

13. Ссылки на ячейки в таблицах MS Word включают:

- ☐ латинские буквы
- ☐ русские буквы
- ☐ арабские цифры
- ☐ римские цифры
- ☐ греческие символы

14. Для вычисления в таблицах MS Word используются формулы, содержащие:

- ☐ математические функции
- ☐ константы
- ☐ встроенные функции

- ☐ знаки математических операций
- ☐ ссылки на блоки текста

15. При слиянии используются следующие документы:

- ☐ итоговый документ
- ☐ основной документ
- ☐ получатель данных
- ☐ источник данных
- ☐ исходный документ

16. Источником данных при слиянии может быть:

- ☐ документ MS Word
- ☐ документ MS Excel
- ☐ документ MS WordPad
- ☐ документ MS Access
- ☐ документ MS Graph

17. Ссылки на ячейки в табличном процессоре MS Excel могут быть:

- ☐ относительными
- ☐ процентными
- ☐ абсолютными
- ☐ смешанными
- ☐ индивидуальными

18. Ячейка таблицы MS Excel может содержать:

- ☐ рисунок
- ☐ текст
- ☐ число
- ☐ формулу
- ☐ дату и время

19. Режимы работы табличного процессора MS Excel:

- ☐ готовности
- ☐ ввода данных
- ☐ командный
- ☐ обычный
- ☐ редактирования

20. Ограничение доступа к электронным таблицам может выполняться на уровне:

- ☐ рабочих книг



- ☐ группы документов
- ☐ формул
- ☐ рабочих листов
- ☐ отдельных ячеек

21. Пункт меню Данные табличного процессора MS Excel позволяет:

- ☐ проводить защиту данных
- ☐ создавать макросы
- ☐ проводить сортировку данных
- ☐ проводить фильтрацию данных
- ☐ проверять орфографию

22. Для запуска макроса можно применять:

- ☐ комбинацию клавиш клавиатуры
- ☐ комбинацию клавиш клавиатуры и экранных кнопок
- ☐ созданные экранные кнопки
- ☐ созданные кнопки панели инструментов
- ☐ текстовую команду

23. При форматировании диаграммы в табличном процессоре MS Excel можно изменить:

- ☐ тип диаграммы
- ☐ исходные данные
- ☐ формат легенды
- ☐ расположение диаграммы
- ☐ формат области построения

24. В плане счетов для некоторого счета установлено ведение аналитического учета в разрезе двух видов субконто – «Материалы» и «Склады». Тогда в программе 1С бухгалтерские итоги по данному счету могут быть получены:

- ☐ отдельно по материалам
- ☐ отдельно по складам
- ☐ по складам в разрезе материалов и складов
- ☐ по материалам в разрезе складов
- ☐ по складам в разрезе материалов

25. В шаблоне типовой операции для некоторого реквизита проводки в параметре «Копирование» установлено наименование этого же реквизита. Данный режим в программе 1С предоставляет пользователю возможность:

- ☐ принудительно копировать значения указанного реквизита из этой же

проводки

☐ принудительно копировать значения указанного реквизита из последующих проводок

☐ принудительно копировать значения указанного реквизита

предшествующих проводок

☐ принудительно копировать значения указанного реквизита из журнала операций

☐ принудительно копировать значения указанного реквизита журнала проводок

26. Данный способ подключения к Интернет обеспечивает наибольшие возможности для доступа к информационным ресурсам:

☐ постоянное соединение по оптоволоконному каналу

☐ удаленный доступ по коммутируемому телефонному каналу

☐ постоянное соединение по выделенному телефонному каналу

☐ терминальное соединение по коммутируемому телефонному каналу

27. Модем, передающий информацию со скоростью 28 800 бит/с, может передать две страницы текста (3 600 байт) в течение...

☐ 1 минуты

☐ 1 часа

☐ 1 секунды

☐ 1 дня

28. Электронная почта (e-mail) позволяет передавать...

☐ только сообщения

☐ только файлы

☐ сообщения и приложенные файлы

☐ видеоизображения

29. Базовым стеком протоколов в Internet является:

☐ HTTP

☐ HTML

☐ TCP

☐ TCP/IP

40. Компьютер, подключенный к Internet, обязательно имеет:

☐ IP-адрес

☐ Web-сервер

☐ домашнюю web-страницу

☐ доменное имя

31. Гиперссылки на web — странице могут обеспечить переход:

- ☐ только в пределах данной web – страницы
- ☐ только на web — страницы данного сервера
- ☐ на любую web — страницу данного региона
- ☐ на любую web — страницу любого сервера Интернет

32. Задан адрес электронной почты в сети Internet: user\_name@int.glasnet.ru.

«Имя» владельца электронного адреса:

- ☐ int.glasnet.ru
- ☐ user\_name
- ☐ glasnet.ru
- ☐ ru

33. Браузеры являются:

- ☐ серверами Интернет
- ☐ антивирусными программами
- ☐ трансляторами языка программирования
- ☐ средством просмотра web-страниц

34. Web-страницы имеют расширение:

- ☐ \*.txt
- ☐ \*.htm
- ☐ \*.doc
- ☐ \*.exe

35. Модем — это устройство, предназначенное для:

- ☐ вывода информации на печать
- ☐ хранения информации
- ☐ обработки информации в данный момент времени
- ☐ передачи информации по каналам связи

36. В качестве гипертекстовых ссылок можно использовать:

- ☐ только слово
- ☐ только картинку
- ☐ любое слово или любую картинку
- ☐ слово, группу слов или картинку

37. Web-страница — это ...

- ☐ документ специального формата, опубликованный в Internet
- ☐ документ, в котором хранится вся информация по сети
- ☐ документ, в котором хранится информация пользователя

□ сводка меню программных продуктов

### **3.2. Промежуточная аттестация**

#### **Типовые вопросы к промежуточной аттестации (Экзамен)**

1. Информация как объект правового регулирования.
2. Меры защиты информации: законодательного, административного, процедурного, программно-технического уровней.
3. Законодательство РФ в области информационной безопасности.
4. Информационная безопасность объекта при осуществлении международного сотрудничества.
5. Виды угроз информационной безопасности.
6. Угрозы конституционным правам и свободам гражданина в области информационной деятельности.
7. Угрозы информационному обеспечению государственной политики Российской Федерации.
8. Угрозы безопасности информационных и телекоммуникационных средств и систем.
9. Внешние и внутренние источники угроз информационной безопасности.
10. Основные виды угроз безопасности субъектов информационных отношений.
11. Основные непреднамеренные и преднамеренные искусственные угрозы.
12. Основные преднамеренные искусственные угрозы.
13. Закон РФ от 21.09.93 "О государственной тайне".
14. Закон РФ от 09.07.2004г. «О коммерческой тайне».
15. Закон РФ от 08.07.2006г. «О персональных данных».
16. «Концепция защиты СВТ и АС от НСД», предназначение, основные понятия и направления.
17. Основные принципы защиты от НСД, изложенные в нормативных документах концепции защиты СВТ и АС.
18. Свойства защищенных автоматизированных систем обработки информации.
19. Специфика возникновения угроз и рисков в открытых сетях.
20. Что понимается под уязвимостью защищенных компьютерных систем?
21. Основные направления обеспечения информационной безопасности в компьютерных системах.
22. Основные понятия безопасности компьютерных систем.

23. Что понимается под лицензированием деятельности в области защиты информации?
24. Перечислить основные мероприятия, позволяющие решить задачу построения системы защиты рабочей станции.
25. Для чего используются системы многоуровневой защиты?
26. Какие вы знаете аспекты защиты информации в системе с разграничением полномочий?
27. Перечислите и дайте характеристику основным методам построения систем защиты с многоуровневым доступом.
28. Какое место занимает механизм подотчетности в политике безопасности и, на какие категории делятся средства подотчетности?
29. Какие проблемы возникают при использовании защиты информации путем ограничения доступа?
30. Какие принципы положены в концепцию построения защищенных систем?
31. Перечислить и дать характеристику основным компонентам технологии построения защищенной компьютерной системы.
32. Каким способом происходит интеграция средств защиты и распространенных приложений в защищенной компьютерной системе?
33. Что понимается под несанкционированным доступом к информации.
34. Перечислить и дать характеристику обобщенным методам защиты от НСД.
35. Что понимается под стойкостью системы идентификации?
36. Что является интегральной характеристикой защищенной системы?
37. Понятие политики безопасности и её основные базовые представления.
38. В каких случаях используют модели безопасности производители защищенных компьютерных систем?
39. Из каких частей состоит ГОСТ Р 15408? 4
40. На каких базовых представлениях основаны модели безопасности?
41. Какие элементы должна включать в себя политика безопасности организации?
42. В чем различие субъекта компьютерной системы от человека-пользователя?
43. Какими качествами должен обладать монитор обращений?
44. Как определяется доверенная система в ГОСТ Р 15408, и по каким критериям

#### **4. Методические материалы, определяющие процедуры оценивания достижения запланированных результатов обучения по дисциплине (модулю)**

##### **Текущая аттестация**

При оценивании устного опроса и участия в дискуссии на семинаре (практическом занятии) учитываются:

- степень раскрытия содержания материала;
- изложение материала (грамотность речи, точность использования терминологии и символики, логическая последовательность изложения материала);
- знание теории изученных вопросов, сформированность и устойчивость используемых при ответе умений и навыков.

Для оценивания результатов обучения в виде знаний используются такие процедуры и технологии как тестирование и опрос на семинарах (практических занятиях).

Для оценивания результатов обучения в виде умений и владений используются следующие процедуры и технологии:

- практические контрольные задания (далее – ПКЗ), включающих одну или несколько задач (вопросов) в виде краткой формулировки действий (комплекса действий), которые следует выполнить, или описание результата, который нужно получить.

По сложности ПКЗ разделяются на простые и комплексные задания.

Простые ПКЗ предполагают решение в одно или два действия. К ним можно отнести: простые ситуационные задачи с коротким ответом или простым действием; несложные задания по выполнению конкретных действий. Простые задания применяются для оценки умений. Комплексные задания требуют многоходовых решений как в типичной, так и в нестандартной ситуациях. Это задания в открытой форме, требующие поэтапного решения и развернутого ответа, в т.ч. задания на индивидуальное или коллективное выполнение проектов, на выполнение практических действий или лабораторных работ. Комплексные практические задания применяются для оценки владений.

Типы практических контрольных заданий:

- задания на установление правильной последовательности, взаимосвязанности действий, выяснения влияния различных факторов на результаты выполнения задания;
- установление последовательности (описать алгоритм выполнения действия),
- нахождение ошибок в последовательности (определить правильный вариант последовательности действий);
- указать возможное влияние факторов на последствия реализации умения и т.д.
- задания на принятие решения в нестандартной ситуации (ситуации выбора, многоальтернативности решений, проблемной ситуации).

Оценивание обучающегося на текущей аттестации осуществляется в соответствии с критериями, представленными в п. 7.1, и носит балльный характер.

## **Промежуточная аттестация**

Форма промежуточной аттестации: Экзамен.

При проведении промежуточной аттестации студент должен ответить на вопросы теоретического характера и практического характера.

При оценивании ответа на вопрос теоретического характера учитывается:

- теоретическое содержание не освоено, знание материала носит фрагментарный характер, наличие грубых ошибок в ответе;
- теоретическое содержание освоено частично, допущено не более двух-трех недочетов;
- теоретическое содержание освоено почти полностью, допущено не более одного-двух недочетов, но обучающийся смог бы их исправить самостоятельно;
- теоретическое содержание освоено полностью, ответ построен по собственному плану.

При оценивании ответа на вопрос практического характера учитывается объем правильного решения.

Основой для определения оценки служит уровень усвоения студентами материала, предусмотренного данной рабочей программой.

Оценивание обучающегося на промежуточной аттестации осуществляется в соответствии с критериями, представленными в п. 2, и носит балльный характер.