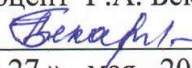


**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ  
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«КАБАРДИНО-БАЛКАРСКИЙ ГОСУДАРСТВЕННЫЙ  
АГРАРНЫЙ УНИВЕРСИТЕТ ИМЕНИ В.М. КОКОВА»**

**Факультет «Экономики и управление»  
Кафедра «Экономика»**

УТВЕРЖДАЮ  
Декан факультета  
доцент Г.А. Бекаров  
  
« 27 » мая 2025 г.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ  
Б1.В.ДВ.03.01 Информационная безопасность предприятия (организации)**

Направление подготовки **38.04.01 Экономика**

Направленность (профиль) **Экономическая безопасность и устойчивое развитие**

Квалификация выпускника: **магистр**

Программа подготовки: **магистратура**

Год обучения **2 (2)**

Семестр **3 (4)**

Форма обучения **очная (заочная)**

Рабочая программа дисциплины **Б1.В.ДВ.03.01 «Информационная безопасность предприятия (организации)»** составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования - магистратура по направлению подготовки 38.04.01 Экономика утвержденного приказом Минобрнауки России от 11 августа 2020 г. № 939 (далее – ФГОС ВО) и рабочего учебного плана подготовки магистров по данному направлению

Составитель рабочей программы:

д.э.н., профессор



В.О. Канчукоев

Рабочая программа рассмотрена на заседании кафедры «Экономика»  
протокол от «22» мая 2025 г. № 10

Заведующий кафедрой,

к.э.н., доцент



С.М. Тхамокова

Одобрено методической комиссией факультета «Экономика и управление»  
Протокол от «23» мая 2025 г. №9  
Председатель МК факультета «Экономика и управление»

к.э.н., доцент



Г.А. Бекаров

Согласовано:

Директор научной библиотеки



И.А. Шогенова

«22» мая 2025 г.

### Цели и задачи дисциплины

**Цель дисциплины:** формирование у обучающихся теоретических знаний и практических навыков в области формирования информационного общества, информационных войн и информационной безопасности, государственной инновационной политики, основных этапов и формах информационно-аналитической работы.

**Задачами дисциплины является:**

- рассмотреть основные понятия, принципы, этапы и особенности сферы информационно-аналитической работы;
- охарактеризовать современное информационное общество, проблемы защиты информации и обеспечения информационной безопасности;
- сформировать у студентов навыки написания информационных обзоров и аналитических справок;
- развить у студентов навыки участия и организации информационно-аналитической работы.

### 2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы.

Код компетенций	Наименование компетенции	Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине
УК-1	Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	ИД-2 <sub>УК-1</sub> Разрабатывает варианты решения проблемной ситуации на основе критического анализа доступных источников информации	<b>Знать:</b> специфику научного знания, его отличия от религиозного, художественного и обыденного знания; главные этапы развития науки; основные проблемы современной науки и приемы самообразования. <b>Уметь:</b> анализировать возникающие в процессе управления мировоззренческие проблемы с точки зрения современных научных парадигм, осмысливать и делать обоснованные выводы из новой научной и учебной литературы, результатов экспериментов, происходящих в мире глобальных событий. <b>Владеть:</b> понятийным аппаратом, навыками научного анализа, управления и методологией научного подхода в научно-исследовательской и практической деятельности, навыками приобретения умений и знаний.
ПК-4	Способен поддерживать устойчивое функционирование интегрированной системы управления рисками	ИД-2 <sub>ПК-4</sub> Анализирует актуальные данные по системе управления рисками, цифровые практики построения системы управления рисками в России и мире	<b>Знать:</b> методические подходы к процедурам актуализации и анализа данных о системе управления рисками в России и в мире. <b>Уметь:</b> проводить анализ сильных и слабых сторон решения, взвешивать и анализировать возможности и риски, нести ответственность за принятые решения, в том числе в нестандартных ситуациях. <b>Владеть:</b> навыками разработки организационно-управленческих решений, анализа возможных последствий, оценки эффективности принятых решений.

### 3. Место дисциплины в структуре ОПОП

Дисциплина Б1.В.ДВ.03.01 «Информационная безопасность предприятия (организации)» входит в часть формируемую участниками образовательных отношений (дисциплины (модули) по выбору) Блока 1 «Дисциплины (модули)», включенных в учебный план направления подготовки 38.04.01 Экономика, направленность «Экономическая безопасность и устойчивое развитие».

**4. Объем дисциплины (модуля) в зачетных единицах и в академических часах, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся**

Учебные занятия	Очная форма обучения				Заочная форма обучения			
	Всего		семестр 3		Всего		семестр 4	
	з.е.	часов	з.е.	часов	з.е.	часов	з.е.	часов
<b>1. Контактная работа, в том числе:</b>	<b>1,03</b>	<b>37(8)*</b>	<b>1,03</b>	<b>37(8)*</b>	<b>0,39</b>	<b>14(4)*</b>	<b>0,39</b>	<b>14(4)*</b>
лекции	0,44	16(4)*	0,44	16(4)*	0,17	6(2)*	0,17	6(2)*
практические занятия	0,44	16(4)*	0,44	16(4)*	0,17	6(2)*	0,17	6(2)*
групповые консультации	0,03	1	0,03	1	0,03	1	0,03	1
контрольные балльно-рейтинговые мероприятия	0,08	3	0,08	3	-	-	-	-
промежуточная аттестация: зачет	0,03	1	0,03	1	0,03	1	0,03	1
<b>2. Самостоятельная работа в том числе:</b>	<b>1,97</b>	<b>71</b>	<b>1,97</b>	<b>71</b>	<b>2,61</b>	<b>94</b>	<b>2,61</b>	<b>94</b>
самостоятельное изучение отдельных тем модуля, подготовка к лабораторным работам, выполнение курсового проекта и т.п.	1,83	66	1,83	66	2,47	89	2,47	89
подготовка к промежуточной аттестации	0,14	5	0,14	5	0,14	5	0,14	5
<b>Общая трудоемкость</b>	<b>3</b>	<b>108</b>	<b>3</b>	<b>108</b>	<b>3</b>	<b>108</b>	<b>3</b>	<b>108</b>

(\*) - занятия, проводимые в интерактивных формах.

**4.1. Содержание дисциплины (модуля) структурированное по темам (разделам) с указанием отведенных на них количества часов и видов учебных занятий (очная форма обучения)**

№ п/п	Разделы дисциплины (название модуля)	Лекции	Практич. занятия	Самост. работа	Всего
1.	Экономическая безопасность предприятия. Источники угроз экономической безопасности предприятия.	2(2)*	2(2)*	8	12(4)*
2.	Служба экономической безопасности предприятия	2(2)*	2(2)*	8	12(4)*
3.	Частная детективная и охранная деятельность в РФ. Физическая защита персонала коммерческого предприятия.	2	2	8	12
4.	Обеспечение сохранности материально-финансовых ценностей. Охрана объектов и обеспечение безопасности перевозок	2	2	8	12
5.	Хищения и методы борьбы с ними	2	2	6	10
6.	Информационная безопасность предприятия	2	2	7	11
7.	Обеспечение безопасности коммерческой деятельности	2	2	7	11
8.	Экономическая безопасность фирмы в условиях риска	2	2	7	11
<b>Итого:</b>		<b>16(4)*</b>	<b>16(4)*</b>	<b>66</b>	<b>98</b>

(\*) - занятия, проводимые в интерактивных формах.

**4.2. Содержание дисциплины (модуля) структурированное по темам (разделам) с указанием отведенного на них количества часов и видов учебных занятий (заочная форма обучения)**

№ п/п	Разделы дисциплины (название модуля)	Лекции	Практич. занятия	Самост. работа	Всего
1.	Экономическая безопасность предприятия. Источники угроз экономической безопасности предприятия.	1(1)*	1(1)*	9	11(2)*
2.	Служба экономической безопасности предприятия	1(1)*	1(1)*	11	13(2)*
3.	Частная детективная и охранная деятельность в РФ. Физическая защита персонала коммерческого предприятия.	1	1	11	13
4.	Обеспечение сохранности материально-финансовых ценностей. Охрана объектов и обеспечение безопасности перевозок	1	1	11	13

5.	хищения и методы борьбы с ними	0,5	0,5	12	13
6.	Информационная безопасность предприятия	0,5	0,5	12	13
7.	Обеспечение безопасности коммерческой деятельности	0,5	0,5	12	13
8.	Экономическая безопасность фирмы в условиях риска	0,5	0,5	11	12
<b>Итого:</b>		<b>6(2)*</b>	<b>6(2)*</b>	<b>89</b>	<b>101</b>

(\*) - занятия, проводимые в интерактивных формах.

## 4.1 Содержание разделов дисциплины (модуля)

### 4.3.1 Лекции

№ п/п	Наименование раздела дисциплины	Номер, тема и содержание лекции	Трудоемкость час.	
			очно	заочно
1.		<p><b>ЛЕКЦИЯ №1. Тема: Экономическая безопасность предприятия. Источники угроз экономической безопасности предприятия.</b></p> <p>Характеристики предпринимательской деятельности. Функциональные составляющие экономической безопасности предприятия. Структуры и особенности российского предпринимательства. Признаки предпринимательства. Предпосылки формирования и развития российского предпринимательства. Угрозы безопасности бизнеса: понятие и виды. Объективные и субъективные негативные воздействия. Внешние и внутренние факторы, затрудняющие функционирование конкретного бизнеса. Типичные причины появления угроз экономической безопасности предприятия.</p>	2(2)*	1(1)*
2.		<p><b>Лекция №2. Тема: Служба экономической безопасности предприятия.</b></p> <p>Служба экономической безопасности предприятия: понятие, задачи, функции. Структура и деятельность службы экономической безопасности. Система безопасности предприятия. Организация режима и охраны. Физическое обеспечение безопасности предприятия. Технические средства обеспечения безопасности предприятия. Организация и осуществление пропускного режима. Разработка инструкций о пропускном режиме. Оборудование КПП и их виды. Пропуск сотрудников, посетителей на объект и отдельные (категорированные) помещения. Порядок пропуска на объект транспортных средств, вывоза продукции, документов и материальных ценностей.</p>	2(2)*	1(1)*
3.		<p><b>Лекция №3. Тема: Частная детективная и охранный деятельность в РФ. Физическая защита персонала коммерческого предприятия.</b></p> <p>Частная охранный деятельность. Смешанные формы детективной и охранный деятельности. Применение специальных средств и огнестрельного оружия при осуществлении частной охранный и детективной деятельности. Контроль и надзор за частной детективной и охранный деятельностью. Виды угроз и способы их реализации. Направления обеспечения безопасности персонала предприятия. Сис-</p>	2	1

		темы обнаружения нарушителя, оборудование мониторинга, системы контроля доступа. Возможные места применения электронных средств контроля доступа. Конфигурация систем обеспечения безопасности.		
4.		<p><b>Лекция №4. Тема: Обеспечение сохранности материально-финансовых ценностей. Охрана объектов и обеспечение безопасности перевозок</b></p> <p>Охрана объектов и помещений. Виды объектов в зависимости от важности, типа охраны и сложности охраны. Технические средства приближения, прикосновения и взлома.</p>	2	1
5.		<p><b>Лекция №5. Тема: Хищения и методы борьбы с ними</b></p> <p>Кражи и их отграничение от грабежей, разбойных нападений, мошенничества, присвоения, растраты и злоупотребления должностными полномочиями. Сферы деятельности, в которых персонал может совершать кражу. Системы мер, препятствующей совершению краж. Виды краж. Критерии проверки персонала на безопасность.</p>	2	0,5
6.		<p><b>Лекция №6. Тема: Информационная безопасность предприятия.</b></p> <p>Источники коммерческой тайны. Типовое положение о коммерческой тайне: понятие, содержание. Виды каналов утечки информации. Организация защиты информации, составляющей коммерческую тайну. Носители коммерческой тайны. Обеспечение безопасности в компьютерных системах предприятия. Компьютерная безопасность. Нецелевые и целевые угрозы информационным системам предприятия. Способы защиты информации в компьютерных системах.</p>	2	0,5
7.		<p><b>Лекция №7. Тема: Обеспечение безопасности коммерческой деятельности .</b></p> <p>Мошенничество и его виды. Структуры российского мошенничества. Мошенник и его жертва. Система мер по защите бизнеса от преступлений внешнего происхождения.</p> <p>Каналы и источники получения деловой информации. Способы ведения деловой разведки, формы и методы получения информации. Сбор информации из открытых и закрытых источников. Информационно-аналитическое обеспечение деловой разведки. Изучение делового партнера.</p>	2	0,5
8.		<p><b>Лекция №8. Тема: Экономическая безопасность фирмы в условиях риска.</b></p> <p>Оценка риска. Причины, заставляющие предпринимателя идти на риск. Управление рисками. Прогнозирование и анализ потерь. Виды потерь: материальные, технические, финансовые, трудовые, потери времени и специальные виды потерь. Деятельность службы безопасности по оценке, прогнозированию и управлению рисками.</p>	2	0,5

		<b>ИТОГО</b>	<b>16(4)*</b>	<b>6(2)*</b>

#### 4.4. Практические занятия

№ п/п	Наименование раздела дисципли- ны	Содержание практического занятия	Трудоемкость, час.	
			очная форма обучения	заочная форма обучения
1.	Экономическая безопасность предприятия. Источники угроз экономической безопасности предприятия.	Практическое занятие 1. Характеристики предпринимательской деятельности. Функциональные составляющие экономической безопасности предприятия. Структуры и особенности российского предпринимательства. Признаки предпринимательства. Предпосылки формирования и развития российского предпринимательства. Угрозы безопасности бизнеса: понятие и виды. Объективные и субъективные негативные воздействия. Внешние и внутренние факторы, затрудняющие функционирование конкретного бизнеса. Типичные причины появления угроз экономической безопасности предприятия.	2(2)*	1(1)*
2.	Служба экономической безопасности предприятия	Практическое занятие 2. Служба экономической безопасности предприятия: понятие, задачи, функции. Структура и деятельность службы экономической безопасности. Система безопасности предприятия. Организация режима и охраны. Физическое обеспечение безопасности. Технические средства обеспечения безопасности предприятия. Организация и осуществление пропускного режима. Разработка инструкций о пропускном режиме. Оборудование КПП и их виды. Пропуск сотрудников, посетителей на объект и отдельные (категорированные) помещения. Порядок пропуска на объект транспортных средств, вывоза продукции, документов и материальных ценностей.	2(2)*	1(1)*
3.	Частная детективная и охранная деятельность в РФ. Физическая защита персонала коммерческого предприятия.	Практическое занятие 3. Частная охранная деятельность. Смешанные формы детективной и охранной деятельности. Применение специальных средств и огнестрельного оружия при осуществлении частной охранной и детективной деятельности. Контроль и надзор за частной детективной и охранной деятельностью. Виды угроз и способы их реализации. Направления обеспечения безопасности персонала предприятия. Системы обнаружения нарушителя, оборудование мониторинга, системы контроля доступа. Возможные места применения электронных средств контроля доступа. Конфигурация систем обеспечения безопасности.	2	1
4.	Обеспечение сохранности материально-финансовых ценностей. Охрана объектов и обеспечение безопасности перевозок	Практическое занятие 4. Охрана объектов и помещений. Виды объектов в зависимости от важности, типа охраны и сложности охраны. Технические средства приближения, прикосновения и взлома.	2	1
5.	Хищения и методы борьбы с ними	Практическое занятие 5. Кражи и их отграничение от грабежей, разбойных нападений, мошенничества, присвоения, растраты и злоупотребления должностными полномочиями. Сферы деятельности, в которых персонал может совершать кражу. Системы мер, препятствующей совершению краж. Виды краж. Критерии проверки персонала на безопасность.	2	0,5
6.	Информационная безопасность предприятия	Практическое занятие 6. Источники коммерческой тайны. Типовое положение о коммерческой тайне: понятие, содержание. Виды каналов утечки информации. Организация защиты информации, составляющей коммерческую тайну. Носители коммерческой тайны. Обеспечение безопасности в компью-	2	0,5

		терных системах предприятия. Компьютерная безопасность. Нецелевые и целевые угрозы информационным системам предприятия. Способы защиты информации в компьютерных системах.		
7.	Обеспечение безопасности коммерческой деятельности	Практическое занятие 7. Мошенничество и его виды. Структуры российского мошенничества. Мошенник и его жертва. Система мер по защите бизнеса от преступлений внешнего происхождения. Каналы и источники получения деловой информации. Способы ведения деловой разведки, формы и методы получения информации. Сбор информации из открытых и закрытых источников. Информационно-аналитическое обеспечение деловой разведки. Изучение делового партнера.	2	0,5
8.	Экономическая безопасность фирмы в условиях риска	Практическое занятие 9. Оценка риска. Причины, заставляющие предпринимателя идти на риск. Управление рисками. Прогнозирование и анализ потерь. Виды потерь: материальные, технические, финансовые, трудовые, потери времени и специальные виды потерь. Деятельность службы безопасности по оценке, прогнозированию и управлению рисками.	2	0,5
<b>ИТОГО</b>			<b>16(4)*</b>	<b>6(2)*</b>

\*Занятия, проводимые в интерактивной форме

### 5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

Для самостоятельной работы обучающихся по дисциплине «Информационная безопасность предприятия (организации)» в научной библиотеке университета имеется достаточное количество учебников и учебных пособий.

На самостоятельную работу при изучении данной дисциплины отводится по очной (заочной) форме обучения соответственно 71 (94) часов, из них 66 (89) часов выделяется на самостоятельное изучение отдельных тем и вопросов. При самостоятельном изучении отдельных тем и вопросов основными видами самостоятельной работы обучающихся являются: проработка учебников, учебных пособий, учебно-методической литературы и информационно-образовательных ресурсов, конспектирование материалов, подготовка к выполнению практических заданий, к опросу, тестированию, к контрольным балльно-рейтинговым мероприятиям и промежуточной аттестации.

На очной форме обучения контроль самостоятельной работы, чаще всего осуществляется перед началом чтения лекции, выполнения лабораторных работ, во время проведения балльно-рейтинговых контрольных мероприятий и промежуточной аттестации.

На заочной форме обучения, контроль самостоятельной работы осуществляется только во время промежуточной аттестации.

Объем часов выделяемых для подготовки к промежуточной аттестации (5 ч. по очной форме и 5 ч. по заочной форме обучения), используется для самостоятельной подготовки обучающихся к зачету. Данный этап является завершающим при изучении дисциплины и контроль самостоятельной работы осуществляется на промежуточной аттестации.

№ темы	Тема и вопросы самостоятельной работы обучающихся	Объем часов очная форма обучения (заочная форма обучения)	Перечень учебно-методического обеспечения	Форма контроля
1.	Экономическая безопасность предприятия. Источники угроз экономической безопасности предприятия. Угрозы безопасности бизнеса: понятие и виды. Объективные и субъективные негативные воздействия. Внешние и внутренние факторы, затрудняющие функционирование конкретного бизнеса.	8(9)	[1,3,6,10]	Подготовка к практическим занятиям, к балльно-рейтинговым контрольным мероприятиям, к зачету. Выполнение заданий, написание рефератов,



				докладов, сообщений, эссе. Ответы на занятиях, контрольных мероприятий и зачете
2.	Служба экономической безопасности предприятия. Пропуск сотрудников, посетителей на объект и отдельные (категорированные) помещения. Порядок пропуска на объект транспортных средств, вывоза продукции, документов и материальных ценностей.	8(11)	[1,2,4,6,11]	Подготовка к практическим занятиям, к балльно-рейтинговым контрольным мероприятиям, к зачету. Выполнение заданий, написание рефератов, докладов, сообщений, эссе. Ответы на занятиях, контрольных мероприятий и зачете
3.	Частная детективная и охранная деятельность в РФ. Физическая защита персонала коммерческого предприятия. Направления обеспечения безопасности персонала предприятия. Системы обнаружения нарушителя, оборудование мониторинга, системы контроля доступа. Возможные места применения электронных средств контроля доступа. Конфигурация систем обеспечения безопасности	8(11)	[1,3,6,13]	Подготовка к практическим занятиям, к балльно-рейтинговым контрольным мероприятиям, к зачету. Выполнение заданий, написание рефератов, докладов, сообщений, эссе. Ответы на занятиях, контрольных мероприятий и зачете
4.	Обеспечение сохранности материально-финансовых ценностей. Охрана объектов и обеспечение безопасности перевозок. Виды объектов в зависимости от важности, типа охраны и сложности охраны. Технические средства приближения, прикосновения и взлома.	8(11)	[1,4,6,10]	Подготовка к практическим занятиям, к балльно-рейтинговым контрольным мероприятиям, к зачету. Выполнение заданий, написание рефератов, докладов, сообщений, эссе. Ответы на занятиях, контрольных мероприятий и зачете
5.	Хищения и методы борьбы с ними. Системы мер, препятствующей совершению краж. Виды краж. Критерии проверки персонала на безопасность.	6(12)	[2,3,5,15]	Подготовка к практическим занятиям, к балльно-рейтинговым контрольным мероприятиям, к зачету. Выполнение заданий, написание рефератов, докладов, сообщений, эссе. Ответы на занятиях, контрольных мероприятий и зачете
6.	Информационная безопасность предприятия. Обеспечение безопасности в компьютерных системах предприятия. Компьютерная безопасность. Нецелевые и целевые угрозы информационным системам предприятия. Способы защиты информации в компьютерных системах.	7(12)	[1,3,6,13]	Подготовка к практическим занятиям, к балльно-рейтинговым контрольным мероприятиям, к зачету. Выполнение заданий, написание рефератов, докладов, сообщений, эссе. Ответы на занятиях, контрольных мероприятий и зачете

7.	Обеспечение безопасности коммерческой деятельности. Сбор информации из открытых и закрытых источников. Информационно-аналитическое обеспечение деловой разведки. Изучение делового партнера.	7(12)	[1,4,6,10]	Подготовка к практическим занятиям, к балльно-рейтинговым контрольным мероприятиям, к зачету. Выполнение заданий, написание рефератов, докладов, сообщений, эссе. Ответы на занятиях, контрольных мероприятиях и зачете
8.	Экономическая безопасность фирмы в условиях риска. Прогнозирование и анализ потерь. Виды потерь: материальные, технические, финансовые, трудовые, потери времени и специальные виды потерь. Деятельность службы безопасности по оценке, прогнозированию и управлению рисками.	7(11)	[1,3,6,10]	Подготовка к практическим занятиям, к балльно-рейтинговым контрольным мероприятиям, к зачету. Выполнение заданий, написание рефератов, докладов, сообщений, эссе. Ответы на занятиях, контрольных мероприятиях и зачете
9.	Подготовка к промежуточной аттестации	5(5)		Подготовка к промежуточной аттестации. Ответ во время сдачи зачета
<b>Итого:</b>		<b>71(94)</b>		

\* Перечень учебно-методического обеспечения приведен в разделе 8.

## 6. Фонд оценочных средств, для проведения текущего и промежуточного контроля знаний обучающихся по дисциплине (модулю)

### 6.1. Перечень компетенций с указанием этапов их формирования при текущем и промежуточном контроле знаний обучающихся

№ модуля	Структурированные модули	Коды формируемых компетенций	Этапы формирования компетенции в процессе освоения дисциплины
	Тема 1. Экономическая безопасность предприятия. Источники угроз экономической безопасности предприятия.	УК-1 ПК-4	1-й рейтинг-контроль. (Балльно-рейтинговые контрольные мероприятия (коллоквиумы, контрольные работы, тесты) подготовка к практическим занятиям)
	Тема 2. Служба экономической безопасности предприятия.		
	Тема 3. Частная детективная и охранный деятельность в РФ. Физическая защита персонала коммерческого предприятия.		
2.	Тема 4. Обеспечение сохранности материально-финансовых ценностей. Охрана объектов и обеспечение безопасности перевозок	УК-1 ПК-4	2-й рейтинг-контроль. (Балльно-рейтинговые контрольные мероприятия (коллоквиумы, контрольные работы, тесты) подготовка к практическим занятиям)
	Тема 5. Хищения и методы борьбы с ними		
	Тема 6. Информационная безопасность предприятия.		
3.	Тема 7. Обеспечение безопасности коммерческой деятельности	УК-1 ПК-4	3-й рейтинг-контроль. (Балльно-рейтинговые контрольные мероприятия (коллоквиумы, контрольные работы, тесты) подготовка к практическим занятиям)
	Тема 8. Экономическая безопасность фирмы в условиях риска		

### 6.2. Показатели и критерии оценивания индикаторов достижения компетенций на раз-

## **личных этапах их формирования, шкалы и процедуры оценивания при текущем и промежуточном контроле знаний обучающихся.**

**Текущий контроль** - это непрерывное отслеживание освоения индикаторов достижения универсальных, общепрофессиональных и профессиональных компетенций по дисциплине.

**Промежуточный контроль** проводится с целью оценки усвоения студентами материала крупного модуля или раздела учебной дисциплины. В течение семестра проводится три таких контрольных мероприятий, согласно календарного учебного графика.

Оценка знаний студентов осуществляется в баллах с учетом:

- оценки (текущего контроля) за работу в семестре (оценки за выполнение контрольных заданий, за выполнение и успешную защиту лабораторных работ, за активное участие в опросе студентов перед началом лекции или в конце ее);

- оценки промежуточных знаний на рейтинговых мероприятиях (ответы на тесты, на контрольные вопросы).

Для определения оценки за работу в семестре и оценки промежуточных знаний на рейтинговых мероприятиях содержательная часть рабочей программы четко структурируется на содержательные модули из которых формируется три блока (модуля), с периодами изучения равными периодам проведения рейтинг-контроля.

Таким образом, устанавливается объем дисциплины, подлежащей оценке качества усвоения в рамках блоков. При этом каждая контрольная точка оценивается в 20 баллов.

Критериями оценки индикатора достижения компетенций являются уровень освоения обучающимися знаний, умений и навыков, которыми они должны обладать при изучении разделов (модулей) дисциплины.

Согласно этих критериев при разработке шкал оценивания автор руководствуется следующим:

**15-20 баллов** – студент получает при **высоком** уровне овладения индикаторами достижения компетенций и освоения знаний, умений и теоретического материала без пробелов; выполнении всех заданий, предусмотренных учебным планом на высоком качественном уровне; сформировании практических навыков, профессионального применения освоенных знаний;

**10-14 баллов** – студент получает при **среднем** уровне овладения индикаторами достижения компетенций и освоении знаний, умений и теоретического материала, когда учебные задания не оценены максимальным числом баллов, и в основном сформированы практические навыки.

**До 10 баллов** – студент получает при **пороговом** уровне овладения индикаторами достижения компетенций и частично с пробелом освоении знаний, умений и теоретического материала, некачественном выполнении учебных заданий, либо они оценены числом баллов близким к минимальному, в случаях не сформирования некоторых практических навыков.

## **7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю)**

### **7.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы**

Рабочей программой дисциплины «Информационная безопасность предприятия (организации)» предусмотрено участие дисциплины в формировании следующих компетенций:

**УК-1** Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий.

**ПК-4** Способен поддерживать устойчивое функционирование интегрированной системы управления рисками.

В процессе освоения образовательной программы по 38.04.01 Экономика компетенции **УК-1, ПК-4** формируются при изучении дисциплин, прохождении практик и ГИА

**Этапы формирования компетенций в процессе освоения образовательной программы  
38.04.01 Экономика, направленность - Экономическая безопасность и устойчивое  
развитие**

<b>Код компетенции</b>	<b>Дисциплины, практики, ГИА, через которые формируется компетенция (компоненты)</b>	<b>Этапы формирования компетенции в процессе освоения образовательной программы*</b>
<b>УК-1</b>	Б1.О.01 Микроэкономика (продвинутый уровень)	1
	Б1.О.07 Методы научных исследований	
	Б1.В.03 Основы теории экономической безопасности	
	ФТД.01 Особенности экономики аграрного производства (продвинутый уровень)	
	Б1.О.03 Современные информационные технологии в экономической науке и практике	2
	Б2.О.02(У) Учебная практика, научно-исследовательская работа(получение первичных навыков научно-исследовательской работы)	
	ФТД.02 Цифровые технологии в АПК	
	Б1.В.07 Цифровая экономическая безопасность	3
	<b>Б1.В.ДВ.03.01 Информационная безопасность предприятия (организации)</b>	
	Б3.01 Подготовка к процедуре защиты и защита выпускной квалификационной	4
<b>ПК-4</b>	Б1.В.05 Управление рисками в системе обеспечения экономической безопасности	2
	Б1.В.07 Цифровая экономическая безопасность	3
	Б1.В.08 Экономика обеспечения безопасности предприятия (организации)	
	<b>Б1.В.ДВ.03.01 Информационная безопасность предприятия (организации)</b>	
	Б2.О.03(Н) Производственная практика, научно-исследовательская работа	
	Б2.О.03(Н) Производственная практика, научно-исследовательская работа	4
	Б2.В.01(Пд) Производственная практика, преддипломная	
	Б3.01 Подготовка к процедуре защиты и защита выпускной квалификационной	

**7.2. Описание показателей индикаторов достижения компетенций на различных этапах их формирования, описание шкал оценивания**

Для оценки знаний, умений, навыков и индикаторов достижения компетенций по дисциплине применяется балльно-рейтинговая система контроля и оценки успеваемости студентов. В основу балльно-рейтинговой системы (БРС) положены принципы, в соответствии с которыми формирование рейтинга студента осуществляется в ходе текущего, промежуточного контроля и промежуточной аттестации знаний.

**Промежуточная аттестация – зачет.**

При модульной системе основным стимулом к регулярной работе студентов является возможность быть освобожденным от зачета (получить их «автоматом»). Для этого студент должен выполнить следующие условия:

- не иметь по промежуточным модулям **0** баллов;

- если студент по итогам текущего рейтинга набрал в семестре **49-54** баллов то он получает, **«автоматом»** оценку - **«хорошо»**, **55** и выше **«отлично»**.

- если студент набрал по итогам текущего рейтинга **49** и более баллов, то он получает зачет «автоматом»

- Максимальная сумма баллов, которую студент может набрать за семестр составляет **100** баллов, из которых на текущий и промежуточный контроль отводится **60** баллов. Оставшиеся **40** баллов - это сумма баллов, которую студент может набрать по результатам промежуточной аттестации (зачет).

**- Индикаторы достижения компетенций\***

Код и наименование индикатора достижения компетенции, этапы освоения	Планируемые результаты обучения	Соответствие индикатора достижения компетенции планируемым результатам обучения и критериям их оценивания			
		минимальный	пороговый	средний	высокий
		0-59	60-69	70-84	85-100
		Оценка			
		не зачтено	зачтено	зачтено	зачтено
ИД-2 <sub>УК-1</sub> Разрабатывает варианты решения проблемной ситуации на основе критического анализа доступных источников информации (3-й этап)	<b>Знать:</b> специфику научного знания, его отличия от религиозного, художественного и обыденного знания; главные этапы развития науки; основные проблемы современной науки и приемы самообразования.	Не знает специфику научного знания, его отличия от религиозного, художественного и обыденного знания; главные этапы развития науки; основные проблемы современной науки и приемы самообразования.	Частично знаком со спецификой научного знания, его отличия от религиозного, художественного и обыденного знания; с главными этапами развития науки; основными проблемами современной науки и приемами самообразования.	Достаточно владеет знаниями о специфике научного знания, его отличия от религиозного, художественного и обыденного знания; главные этапы развития науки; основные проблемы современной науки и приемы самообразования.	В полной мере владеет знаниями о специфике научного знания, его отличия от религиозного, художественного и обыденного знания; главные этапы развития науки; основные проблемы современной науки и приемы самообразования.
	<b>Уметь:</b> анализировать возникающие в процессе управления мировоззренческие проблемы с точки зрения современных научных парадигм, осмысливать и делать обоснованные выводы из новой научной и учебной литературы, результатов экспериментов, происходящих в мире глобальных событий.	Не обладает умениями анализировать возникающие в процессе управления мировоззренческие проблемы с точки зрения современных научных парадигм, осмысливать и делать обоснованные выводы из новой научной и учебной литературы, результатов экспериментов, происходящих в мире глобальных событий.	Частично обладает умениями анализировать возникающие в процессе управления мировоззренческие проблемы с точки зрения современных научных парадигм, осмысливать и делать обоснованные выводы из новой научной и учебной литературы, результатов экспериментов, происходящих в мире глобальных событий.	Умеет хорошо анализировать возникающие в процессе управления мировоззренческие проблемы с точки зрения современных научных парадигм, осмысливать и делать обоснованные выводы из новой научной и учебной литературы, результатов экспериментов, происходящих в мире глобальных событий.	В полной мере может анализировать возникающие в процессе управления мировоззренческие проблемы с точки зрения современных научных парадигм, осмысливать и делать обоснованные выводы из новой научной и учебной литературы, результатов экспериментов, происходящих в мире глобальных событий.

	<b>Владеть:</b> понятийным аппаратом, навыками научного анализа, управления и методологией научного подхода в научно-исследовательской и практической деятельности, навыками приобретения умений и знаний.	Не владеет понятийным аппаратом, навыками научного анализа, управления и методологией научного подхода в научно-исследовательской и практической деятельности, навыками приобретения умений и знаний.	Не в полной мере владеет понятийным аппаратом, навыками научного анализа, управления и методологией научного подхода в научно-исследовательской и практической деятельности, навыками приобретения умений и знаний.	Владеет хорошо понятийным аппаратом, навыками научного анализа, управления и методологией научного подхода в научно-исследовательской и практической деятельности, навыками приобретения умений и знаний.	В полной мере владеет понятийным аппаратом, навыками научного анализа, управления и методологией научного подхода в научно-исследовательской и практической деятельности, навыками приобретения умений и знаний.
ИД-2 ПК-4 Анализирует актуальные данные по системе управления рисками, цифровые практики построения системы управления рисками в России и мире	<b>Знать:</b> методические подходы к процедурам актуализации и анализа данных о системе управления рисками в России и в мире.	Не знает методические подходы к процедурам актуализации и анализа данных о системе управления рисками в России и в мире.	Частично знаком с методическими подходами к процедурам актуализации и анализа данных о системе управления рисками в России и в мире.	Знает на хорошем уровне методические подходы к процедурам актуализации и анализа данных о системе управления рисками в России и в мире.	В полной мере знает методические подходы к процедурам актуализации и анализа данных о системе управления рисками в России и в мире.
	<b>Уметь:</b> проводить анализ сильных и слабых сторон решения, взвешивать и анализировать возможности и риски, нести ответственность за принятые решения, в том числе в нестандартных ситуациях.	Не обладает умениями проводить анализ сильных и слабых сторон решения, взвешивать и анализировать возможности и риски, нести ответственность за принятые решения, в том числе в нестандартных ситуациях.	Частично обладает умениями проводить анализ сильных и слабых сторон решения, взвешивать и анализировать возможности и риски, нести ответственность за принятые решения, в том числе в нестандартных ситуациях.	Умеет хорошо проводить анализ сильных и слабых сторон решения, взвешивать и анализировать возможности и риски, нести ответственность за принятые решения, в том числе в нестандартных ситуациях.	На высоком уровне обладает умением проводить анализ сильных и слабых сторон решения, взвешивать и анализировать возможности и риски, нести ответственность за принятые решения, в том числе в нестандартных ситуациях.
	<b>Владеть:</b> навыками разработки организационно-управленческих решений, анализа возможных последствий, оценки эффективности принятых решений.	Не владеет навыками разработки организационно-управленческих решений, анализа возможных последствий, оценки эффективности принятых решений.	Не в полной мере владеет навыками разработки организационно-управленческих решений, анализа возможных последствий, оценки эффективности принятых решений.	Способен обеспечить на хорошем уровне разработку организационно-управленческих решений, анализа возможных последствий, оценки эффективности принятых решений.	Владеет на высоком уровне навыками разработки организационно-управленческих решений, анализа возможных последствий, оценки эффективности принятых решений.

Для допуска к зачету обучающийся должен набрать в ходе текущего и промежуточного контроля не менее **40** баллов. Если эта сумма меньше **30** баллов, то обучающийся не допускается к зачету. Если эта сумма не меньше **30**, то путем дополнительного опроса (собеседова-

ние, контрольная работа, тест, реферат), она может быть повышена до **40** баллов.

Для допуска к зачету обучающемуся необходимо восстановить пробелы, как по текущему, так и по промежуточному контролю. На зачете студент может получить **20–40** баллов. Максимальный балл при каждой повторной пересдаче уменьшается на **10** баллов. Если ответы студента оцениваются суммой баллов менее **20**, то ему выставляется **0** баллов.

### Критерии оценивания результатов обучения

Оценка	Шкала оценивания	Критерии оценивания
Высокий уровень «5» (зачтено)	85-100	оценку « <b>отлично</b> » заслуживает студент, освоивший знания, умения, компетенции и теоретический материал без пробелов; выполнивший все предусмотренные задания на высоком качественном уровне; практические навыки профессионального применения освоенных знаний сформированы.
Средний уровень «4» (зачтено)	70-84	оценку « <b>хорошо</b> » заслуживает студент, практически полностью освоивший знания, умения, компетенции и теоретический материал, учебные задания не оценены максимальным числом баллов, в основном сформировал практические навыки.
Пороговый уровень «3» (зачтено)	60-69	оценку « <b>удовлетворительно</b> » заслуживает студент, частично с пробелами освоивший знания, умения, компетенции и теоретический материал, многие учебные задания либо не выполнил, либо они оценены числом баллов близким к минимальному, некоторые практические навыки не сформированы.
Минимальный уровень «2» (не зачтено)	0-59	оценку « <b>неудовлетворительно</b> » заслуживает студент, не освоивший знания, умения, компетенции и теоретический материал, учебные задания не выполнил, практические навыки не сформированы.

### 7.3. Контрольные задания или иные материалы, необходимые для оценки результатов освоения индикаторов достижения компетенции ИД-2ук-1, ИД-2пк-4 в процессе освоения образовательной программы

#### 7.3.1. Примерная тематика рефератов

1. Корпоративная культура, информационное обеспечение ее формирования в организации.
2. Контент-анализ и его использование при проведении информационно-аналитической работы.
3. Система информационно-аналитического обеспечения в сфере безопасности
4. Информационно-аналитические центры по проблемам информационной безопасности РФ.
5. Информационно-аналитическое обеспечение деятельности служб информационной безопасности.
6. Информационно-аналитическое обеспечение деятельности служб комплексной безопасности.
7. Система информационного обеспечения деятельности в разных сферах.
8. Особенности современных антивирусных программ.
9. Интернет – альтернативная сеть массовой коммуникации.
10. Информационно-аналитическая работа в команде.
11. «Мозговой штурм» как способ продуцирования нового знания.
12. Тайм-менеджмент.
13. Информация и коммуникация в системах информационно-аналитической деятельности.
14. Информационно-аналитическая работа в информационных войнах .

#### 7.3.2. Тесты для текущего и промежуточного контроля знаний обучающихся Раздел 1. Предпочтения и выбор потребителя

- 1. Кто является основным ответственным за определение уровня классификации информации?**
- A. Руководитель среднего звена
  - B. Высшее руководство
  - C. Владелец
  - D. Пользователь
- 2. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?**
- A. Сотрудники
  - B. Хакеры
  - C. Атакующие
  - D. Контрагенты (лица, работающие по договору)
- 3. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?**
- A. Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования
  - B. Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации
  - C. Улучшить контроль за безопасностью этой информации
  - D. Снизить уровень классификации этой информации
- 4. Что самое главное должно продумать руководство при классификации данных?**
- A. Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным
  - B. Необходимый уровень доступности, целостности и конфиденциальности
  - C. Оценить уровень риска и отменить контрмеры
  - D. Управление доступом, которое должно защищать данные
- 5. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?**
- A. Владельцы данных
  - B. Пользователи
  - C. Администраторы
  - D. Руководство
- 6. Что такое процедура?**
- A. Правила использования программного и аппаратного обеспечения в компании
  - B. Пошаговая инструкция по выполнению задачи
  - C. Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах
  - D. Обязательные действия
- 7. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?**
- A. Поддержка высшего руководства
  - B. Эффективные защитные меры и методы их внедрения
  - C. Актуальные и адекватные политики и процедуры безопасности
  - D. Проведение тренингов по безопасности для всех сотрудников
- 8. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?**
- A. Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски
  - B. Когда риски не могут быть приняты во внимание по политическим соображениям
  - C. Когда необходимые защитные меры слишком сложны
  - D. Когда стоимость контрмер превышает ценность актива и потенциальные потери
- 9. Что такое политики безопасности?**
- A. Пошаговые инструкции по выполнению задач безопасности
  - B. Общие руководящие требования по достижению определенного уровня безопасности
  - C. Широкие, высокоуровневые заявления руководства



D. Детализированные документы по обработке инцидентов безопасности

**10. Какая из приведенных техник является самой важной при выборе конкретных защитных мер?**

A. Анализ рисков

B. Анализ затрат / выгоды

C. Результаты ALE

D. Выявление уязвимостей и угроз, являющихся причиной риска

**11. Что лучше всего описывает цель расчета ALE?**

A. Количественно оценить уровень безопасности среды

B. Оценить возможные потери для каждой контрмеры

C. Количественно оценить затраты / выгоды

D. Оценить потенциальные потери от угрозы в год

**12. Тактическое планирование – это:**

A. Среднесрочное планирование

B. Долгосрочное планирование

C. Ежедневное планирование

D. Планирование на 6 месяцев

**13. Что является определением воздействия (exposure) на безопасность?**

A. Нечто, приводящее к ущербу от угрозы

B. Любая потенциальная опасность для информации или систем

C. Любой недостаток или отсутствие информационной безопасности

D. Потенциальные потери от угрозы

**14. Эффективная программа безопасности требует сбалансированного применения:**

A. Технических и нетехнических методов

B. Контрмер и защитных механизмов

C. Физической безопасности и технических средств защиты

D. Процедур безопасности и шифрования

**15. Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют:**

A. Внедрение управления механизмами безопасности

B. Классификацию данных после внедрения механизмов безопасности

C. Уровень доверия, обеспечиваемый механизмом безопасности

D. Соотношение затрат / выгод

**16. Какое утверждение является правильным, если взглянуть на разницу в целях безопасности для коммерческой и военной организации?**

A. Только военные имеют настоящую безопасность

B. Коммерческая компания обычно больше заботится о целостности и доступности данных, а военные – о конфиденциальности

C. Военным требуется больший уровень безопасности, т.к. их риски существенно выше

D. Коммерческая компания обычно больше заботится о доступности и конфиденциальности данных, а военные – о целостности

**17. Как рассчитать остаточный риск?**

A. Угрозы x Риски x Ценность актива

B. (Угрозы x Ценность актива x Уязвимости) x Риски

C. SLE x Частоту = ALE

D. (Угрозы x Уязвимости x Ценность актива) x Недостаток контроля

**18. Что из перечисленного не является целью проведения анализа рисков?**

A. Делегирование полномочий

B. Количественная оценка воздействия потенциальных угроз

C. Выявление рисков

D. Определение баланса между воздействием риска и стоимостью необходимых контрмер

**19. Что из перечисленного не является задачей руководства в процессе внедрения и сопровождения безопасности?**

- A. Поддержка
- B. Выполнение анализа рисков
- C. Определение цели и границ
- D. Делегирование полномочий

**20. Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?**

- A. Чтобы убедиться, что проводится справедливая оценка
- B. Это не требуется. Для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ
- C. Поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа
- D. Поскольку люди в различных подразделениях сами являются одной из причин рисков, они должны быть ответственны за их оценку

**21. Что является наилучшим описанием количественного анализа рисков?**

- A. Анализ, основанный на сценариях, предназначенный для выявления различных угроз безопасности
- B. Метод, используемый для точной оценки потенциальных потерь, вероятности потерь и рисков
- C. Метод, сопоставляющий денежное значение с каждым компонентом оценки рисков
- D. Метод, основанный на суждениях и интуиции

**22. Почему количественный анализ рисков в чистом виде не достижим?**

- A. Он достижим и используется
- B. Он присваивает уровни критичности. Их сложно перевести в денежный вид.
- C. Это связано с точностью количественных элементов
- D. Количественные измерения должны применяться к качественным элементам

**23. Если используются автоматизированные инструменты для анализа рисков, почему все равно требуется так много времени для проведения анализа?**

- A. Много информации нужно собрать и ввести в программу
- B. Руководство должно одобрить создание группы
- C. Анализ рисков не может быть автоматизирован, что связано с самой природой оценки
- D. Множество людей должно одобрить данные

**24. Какой из следующих законодательных терминов относится к компании или человеку, выполняющему необходимые действия, и используется для определения обязательств?**

- A. Стандарты
- B. Должный процесс (Due process)
- C. Должная забота (Due care)
- D. Снижение обязательств

**25. Что такое CobiT и как он относится к разработке систем информационной безопасности и программ безопасности?**

- A. Список стандартов, процедур и политик для разработки программы безопасности
- B. Текущая версия ISO 17799
- C. Структура, которая была разработана для снижения внутреннего мошенничества в компаниях
- D. Открытый стандарт, определяющий цели контроля

**26. Из каких четырех доменов состоит CobiT?**

- A. Планирование и Организация, Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка
- B. Планирование и Организация, Поддержка и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка
- C. Планирование и Организация, Приобретение и Внедрение, Сопровождение и Покупка, Мониторинг и Оценка
- D. Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка

### **7.3.3. Задания для подготовки к балльно-рейтинговым контрольным мероприятиям**

#### **1-й рейтинг-контроль**

1. Характеристики предпринимательской деятельности.
2. Функциональные составляющие экономической безопасности предприятия.
3. Структуры и особенности российского предпринимательства.
4. Признаки предпринимательства.
5. Предпосылки формирования и развития российского предпринимательства.
6. Угрозы безопасности бизнеса: понятие и виды.
7. Объективные и субъективные негативные воздействия.
8. Внешние и внутренние факторы, затрудняющие функционирование конкретного бизнеса.
9. Типичные причины появления угроз экономической безопасности предприятия.
10. Служба экономической безопасности предприятия: понятие, задачи, функции.
11. Структура и деятельность службы экономической безопасности.
12. Система безопасности предприятия. Организация режима и охраны. Физическое обеспечение безопасности.
13. Технические средства обеспечения безопасности предприятия.
14. Организация и осуществление пропускного режима. Разработка инструкций о пропускном режиме.
15. Оборудование КПП и их виды. Пропуск сотрудников, посетителей на объект и отдельные (категоризированные) помещения. Порядок пропуска на объект транспортных средств, вывоза продукции, документов и материальных ценностей.

#### **2-й рейтинг-контроль**

1. Частная охранная деятельность. Смешанные формы детективной и охранной деятельности.
2. Применение специальных средств и огнестрельного оружия при осуществлении частной охранной и детективной деятельности. Контроль и надзор за частной детективной и охранной деятельностью.
3. Виды угроз и способы их реализации. Направления обеспечения безопасности персонала предприятия.
4. Системы обнаружения нарушителя, оборудование мониторинга, системы контроля доступа. Возможные места применения электронных средств контроля доступа. Конфигурация систем обеспечения безопасности.
5. Охрана объектов и помещений. Виды объектов в зависимости от важности, типа охраны и сложности охраны.
6. Технические средства приближения, прикосновения и взлома.
7. Кражи и их отграничение от грабежей, разбойных нападений, мошенничества, присвоения, растраты и злоупотребления должностными полномочиями.
8. Сферы деятельности, в которых персонал может совершать кражу.
9. Системы мер, препятствующей совершению краж. Виды краж.
10. Критерии проверки персонала на безопасность.
11. Источники коммерческой тайны. Типовое положение о коммерческой тайне: понятие, содержание.
12. Виды каналов утечки информации.
13. Организация защиты информации, составляющей коммерческую тайну. Носители коммерческой тайны.
14. Обеспечение безопасности в компьютерных системах предприятия. Компьютерная безопасность.

Нецелевые и целевые угрозы информационным системам предприятия.

#### **3-й рейтинг-контроль**

1. Способы защиты информации в компьютерных системах.
2. Мошенничество и его виды. Структуры российского мошенничества.
3. Мошенник и его жертва. Система мер по защите бизнеса от преступлений внеш-

него происхождения.

4. Каналы и источники получения деловой информации.
5. Способы ведения деловой разведки, формы и методы получения информации. Сбор информации из открытых и закрытых источников.
6. Информационно-аналитическое обеспечение деловой разведки. Изучение делового партнера.
7. Роль персонала в обеспечении безопасности предприятия.
8. Принципы организации профессионального отбора. Проблемы работы с персоналом в коммерческой структуре.
9. Правила и порядок заполнения документов при приеме на работу.
10. Применение психодиагностических методик в исследовании персонала предприятия. Процесс увольнения кадров.
11. Оценка риска. Причины, заставляющие предпринимателя идти на риск. Управление рисками.
12. Прогнозирование и анализ потерь. Виды потерь: материальные, технические, финансовые, трудовые, потери времени и специальные виды потерь.
13. Деятельность службы безопасности по оценке, прогнозированию и управлению рисками.

#### **7.3.4. Перечень вопросов выносимых на промежуточную аттестацию**

1. Характеристики предпринимательской деятельности.
2. Функциональные составляющие экономической безопасности предприятия.
3. Структуры и особенности российского предпринимательства.
4. Признаки предпринимательства.
5. Предпосылки формирования и развития российского предпринимательства.
6. Угрозы безопасности бизнеса: понятие и виды.
7. Объективные и субъективные негативные воздействия.
8. Внешние и внутренние факторы, затрудняющие функционирование конкретного бизнеса.
9. Типичные причины появления угроз экономической безопасности предприятия.
10. Служба экономической безопасности предприятия: понятие, задачи, функции.
11. Структура и деятельность службы экономической безопасности.
12. Система безопасности предприятия. Организация режима и охраны. Физическое обеспечение безопасности.
13. Технические средства обеспечения безопасности предприятия.
14. Организация и осуществление пропускного режима. Разработка инструкций о пропускном режиме.
15. Оборудование КПП и их виды. Пропуск сотрудников, посетителей на объект и отдельные (категоризированные) помещения. Порядок пропуска на объект транспортных средств, вывоза продукции, документов и материальных ценностей.
16. Частная охранная деятельность. Смешанные формы детективной и охранной деятельности.
17. Применение специальных средств и огнестрельного оружия при осуществлении частной охранной и детективной деятельности. Контроль и надзор за частной детективной и охранной деятельностью.
18. Виды угроз и способы их реализации. Направления обеспечения безопасности персонала предприятия.
19. Системы обнаружения нарушителя, оборудование мониторинга, системы контроля доступа. Возможные места применения электронных средств контроля доступа. Конфигурация систем обеспечения безопасности.
20. Охрана объектов и помещений. Виды объектов в зависимости от важности, типа охраны и сложности охраны.
21. Технические средства приближения, прикосновения и взлома.
22. Кражи и их отграничение от грабежей, разбойных нападений, мошенничества,

- присвоения, растраты и злоупотребления должностными полномочиями.
23. Сферы деятельности, в которых персонал может совершать кражу.
  24. Системы мер, препятствующей совершению краж. Виды краж.
  25. Критерии проверки персонала на безопасность.
  26. Источники коммерческой тайны. Типовое положение о коммерческой тайне: понятие, содержание.
  27. Виды каналов утечки информации.
  28. Организация защиты информации, составляющей коммерческую тайну. Носители коммерческой тайны.
  29. Обеспечение безопасности в компьютерных системах предприятия. Компьютерная безопасность.
  30. Нецелевые и целевые угрозы информационным системам предприятия.
  31. Способы защиты информации в компьютерных системах.
  32. Мошенничество и его виды. Структуры российского мошенничества.
  33. Мошенник и его жертва. Система мер по защите бизнеса от преступлений внешнего происхождения.
  34. Каналы и источники получения деловой информации.
  35. Способы ведения деловой разведки, формы и методы получения информации. Сбор информации из открытых и закрытых источников.
  36. Информационно-аналитическое обеспечение деловой разведки. Изучение делового партнера.
  37. Роль персонала в обеспечении безопасности предприятия.
  38. Принципы организации профессионального отбора. Проблемы работы с персоналом в коммерческой структуре.
  39. Правила и порядок заполнения документов при приеме на работу.
  40. Применение психодиагностических методик в исследовании персонала предприятия. Процесс увольнения кадров.
  41. Оценка риска. Причины, заставляющие предпринимателя идти на риск. Управление рисками.
  42. Прогнозирование и анализ потерь. Виды потерь: материальные, технические, финансовые, трудовые, потери времени и специальные виды потерь.
  43. Деятельность службы безопасности по оценке, прогнозированию и управлению рисками.

#### **7.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций**

Методическими материалами, определяющими процедуру оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих индикаторы достижений компетенций являются внутривузовские локальные нормативные акты: «Положение о балльно-рейтинговой системе контроля и оценки успеваемости студентов» и «Положение о промежуточной аттестации обучающихся».

График проведения рейтинговых контрольных мероприятий и даты проведения промежуточной аттестации, по курсам и семестрам, отражены в утвержденных проректором по УР календарных учебных графиках и расписаниях промежуточной аттестации по направлению подготовки (специальности), которые размещаются на информационных стендах факультетов и на сайте университета в установленные сроки.

### **8. Перечень основной и дополнительной учебной литературы**

#### **Основная литература:**

1. Голиков, А.М. Защита информации в инфокоммуникационных системах и сетях : учебное пособие / А.М. Голиков ; Томский Государственный университет систем управления и радиоэлектроники (ТУСУР). – Томск : Томский государственный университет систем управления и радиоэлектроники, 2015. – 284 с. : схем., табл., ил. – Ре-

жим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=480637>  
– Библиогр. в кн. – Текст : электронный

2. Раченко, Т. А. Информационная безопасность : учебно-методическое пособие / Т. А. Раченко. — Тольятти : ТГУ, 2024. — 135 с. — ISBN 978-5-8259-1612-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book>.
3. Ищейнов, В. Я. Информационная безопасность и защита информации : теория и практика : учебное пособие : [16+] / В. Я. Ищейнов. — Москва ; Берлин : Директ-Медиа, 2020. — 271 с. : схем., табл. — Режим доступа: по подписке. — URL: <https://biblioclub.ru/> — Текст : электронный.
4. Моргунов, А.В. Информационная безопасность : учебно-методическое пособие : [16+] / А.В. Моргунов ; Новосибирский государственный технический университет. — Новосибирск : Новосибирский государственный технический университет, 2019. — 83 с. : ил., табл. — Режим доступа: по подписке. — URL:

#### **Дополнительная литература:**

5. Андрианов В.В. и др. Обеспечение информационной безопасности бизнеса. - М.: ЦИПСИР, Альпина паблишерз, 2011. – 289 с.
6. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А./Основы информационной безопасности/М.: Телеком - горячая линия, 2010. – 276 с.
7. Курилло А.П. и др./ Обеспечение информационной безопасности бизнеса/ «БДЦ-Пресс», 2010. – 348 с.
8. Лондон Дж., Лондон К./Управление информационными системами/ «Питер», 2010. – 694 с.
9. Сборник/Безопасность России. Информационная безопасность/МГФ «Знание», 2010. – 177 с.
10. Стрельцов А.А./Обеспечение информационной безопасности России/ МЦНМО, 2011. – 379 с.

#### **9. Перечень современных профессиональных баз данных и информационных справочных систем**

- **ЭБС «Издательства Лань»**  
**Коллекция «Единая профессиональная база знаний для аграрных вузов»**  
**ООО «Издательство Лань».**  
Лицензионный договор № 003/2025-44ФЗ от 22.05.25 г сроком на 1 год  
<http://e.lanbook.com/>
- **Сетевая электронная библиотека**  
**ООО «ЭБС ЛАНЬ»**  
Договор № СЭБ НВ-164 от 17.12.2019 г. – бессрочный  
<http://e.lanbook.com/>  
<http://seb.e.lanbook.com/>
- **ЭБС «Университетская библиотека online». Базовая часть**  
**ООО «Директ-Медиа»**  
Контракт № 51-04/2025 от 22.05.2025 г сроком на 1 год  
<http://biblioclub.ru>
- **Научная электронная библиотека e-LIBRARY.RU (SCIENCE INDEX)**  
**ООО Научная электронная библиотека.**  
Лицензионный договор № SIO-2114/2025 от 06.05.2025 сроком на 1 год  
<http://elibrary.ru>
- **Сертификат ИТС ПО САБ ИРБИС64**  
**ООО «Эй Ви Ди - Систем»**  
Договор № А-12933 от 12.04.2024 г. сроком на 1 год

**10. Методические указания для обучающихся по освоению дисциплины**

При изучении дисциплины «Информационная безопасность предприятия (организации)» необходимо учитывать особенность Федеральных государственных образовательных стандартов высшего образования – их компетентностную ориентацию, которая нацелена не на сумму усвоенной информации, а на способность человека действовать в различных ситуациях.

Главной целью реализации компетентностного подхода является формирования и развития профессиональных навыков студентов, увеличение доли участия обучающихся в учебном процессе через широкое использование активных и интерактивных форм проведения занятий (семинаров в диалоговом режиме, дискуссий, компьютерных симуляций, долевых и ролевых игр, разбор конкретных ситуаций, психологических и иных тренингов, групповых дискуссий, результатов работы студенческих исследовательских групп, вузовских и межвузовских телеконференций) в сочетании с внеаудиторной работой.

Дисциплина дисциплины «Информационная безопасность предприятия (организации)» рассчитана на изучение в один семестр и заканчивается зачетом с оценкой.

На лекциях студенту рекомендуется внимательно слушать учебный материал, записывать основные моменты, идеи, пытаться сразу понять главные положения темы, а если что не ясно – делать соответствующие пометки. После лекции во внеурочное время целесообразно прочитать записанный материал с целью его усвоения и выяснения непонятных вопросов.

Раздел «Самостоятельная работа» информирует обучающихся, какие вопросы раздела (модуля) выносятся на самостоятельное изучение, об их учебно-методическом обеспечении (учебники, учебные пособия, методические указания, рекомендуемые страницы и т.д.).

Степень усвояемости вопросов самостоятельной работы определяется при текущем и промежуточном контролях и при промежуточной аттестации.

Для студентов заочной формы обучения, после окончания предыдущей сессии, практикуется установочные занятия, где они ознакомились с целями и задачами изучения дисциплины, с перечнем вопросов которые они должны изучать для обладания запланированными в рабочей программе компетенциями. Студенту следует тщательно готовиться к модульному тестированию, контрольным работам, контрольным опросам, прорабатывая конспект лекций и рекомендуемую литературу.

**11. Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства****11.1 Лицензионное программное обеспечение**

AutoDesk AutoCad 2012 Education Product Standalone б/н

**Антиплагиат.VY3 5.0 Модуль поиска «Объединенная коллекция 2020»** лицензионный договор № 10023 от 12.05.2025 г. сроком на 1 год

Kaspersky Endpoint Security для бизнеса – Стандартный Russian Edition № лицензии 26EC-241021-134643-810-2826, договор № 651/А от 18.10.2024 г. до 31.10.2025

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

№ п.п.	Вид учебной работы	Наименование оборудованных учебных кабинетов, лабораторий	Перечень оборудования и технических средств обучения
1.	Лекционные занятия	Аудитории (№№ 323, 324, 310) для проведения занятий лекционного типа в соответ-	Доска аудиторная, специализированная мебель, экран настенный, проектор, ноутбук

		ствии с перечнем аудиторного фонда	
2.	Практические занятия	Аудитории (№№ 323, 324, 310) для проведения занятий лекционного типа в соответствии с перечнем аудиторного фонда	Доска аудиторная, специализированная мебель, экран настенный, проектор, ноутбук
3.	Самостоятельная работа	Учебная аудитория (компьютерный класс с выходом в Интернет), для организации самостоятельной работы обучающихся; читальный зал научной библиотеки	Доска аудиторная, специализированная мебель, компьютера с выходом в интернет