

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ  
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
СТАВРОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ  
УНИВЕРСИТЕТ**

**УТВЕРЖДАЮ**

И.о. декана экономического факультета,

д.э.н., профессор

Кусакина О.Н.

«24» мая 2022 г.

**Рабочая программа дисциплины**

**Б1.В.ДВ.03.02 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**

Шифр и наименование дисциплины по учебному плану

**38.03.01 Экономика**

Код и наименование направления подготовки

**Экономика предприятий и организаций**

Наименование профиля подготовки

**бакалавр**

Квалификация выпускника

**Очная, очно-заочная**

Форма обучения

**2022**

год набора на ОП

Ставрополь, 2022

## 1. Цель дисциплины

Целью изучения дисциплины «Информационная безопасность» является формирование у студентов бакалавриата теоретических знаний и практических навыков по защищённому сбору, обработке и мониторингу исходных данных, необходимых для проведения анализа и планирования показателей производственной, коммерческой и финансово-экономической деятельности организации. Студенты знакомятся с понятием информационная безопасность и защита информации, методами и средствами обеспечения информационной безопасности производственной, коммерческой и финансово-экономической информации организации, порядком их применения в предстоящей профессиональной деятельности.

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

Процесс изучения дисциплины направлен на формирование следующих компетенций ОП ВО и овладение следующими результатами обучения по дисциплине:

Код и наименование компетенции	Коды и наименования индикаторов достижения компетенций	Перечень планируемых результатов обучения по дисциплине
ПК-1 Сбор, мониторинг и обработка данных для проведения расчетов экономических показателей организации	ПК-1.1 Способен выполнять работы по сбору, обработке и мониторингу исходных данных, необходимых для проведения анализа и планирования показателей производственной, коммерческой и финансово-экономической деятельности организации.	<p><b>Знания:</b> методов и приемов сбора, обработки и мониторинга исходных данных, необходимых для проведения анализа и планирования показателей производственной, коммерческой и финансово-экономической деятельности организации с учетом требований информационной безопасности (ПК-1.1);</p> <p><b>Умения:</b> осуществлять работы по сбору, обработке и мониторингу исходных данных, необходимых для проведения анализа и планирования показателей производственной, коммерческой и финансово-экономической деятельности организации с учетом требований информационной безопасности (ПК-1.1);</p> <p><b>Навыки и/или трудовые действия:</b> сбора, обработки и мониторинга показателей производственной, коммерческой и финансово-экономической деятельности организации с учетом требований информационной безопасности (ПК-1.1).</p>
ПК-2 Расчет и анализ экономических показателей результатов деятельности организации	ПК-2.1 Обосновывает и применяет статистические, экономико-математические, маркетинговые методы исследования внешней среды и деятельности организации, проводит расчеты финансово-экономических показателей, в т.ч. с использованием типовых методик и нормативно-правовых актов.	<p><b>Знания:</b> методов проведения статистических, экономико-математических, маркетинговых исследований внешней среды и деятельности организации с учетом требований информационной безопасности (ПК-2.1);</p> <p><b>Умения:</b> проводить статистические, экономико-математические, маркетинговые методы исследования внешней среды и деятельности организации с учетом требований информационной безопасности (ПК-2.1);</p> <p><b>Навыки и/или трудовые действия:</b> решения типовых задач проведения расчетов финансово-экономических показателей организации, в т.ч. с использованием типовых методик и нормативно-правовых актов (ПК-1.2).</p>

### 3. Место дисциплины в структуре образовательной программы

Дисциплина Б1.В.ДВ.03.02 «Информационная безопасность» является дисциплиной по выбору обязательной части, формируемой участником образовательных отношений бакалавриата.

Изучение дисциплины осуществляется:

- для студентов очной формы обучения – в 7 семестре;
- для студентов очно-заочной формы обучения – в 8 семестре.

Для освоения дисциплины «Информационная безопасность» студенты используют знания, умения и навыки, сформированные в процессе изучения дисциплин 1-7(8) семестров, указанных в пункте 7.1.

Освоение дисциплины «Информационная безопасность» является необходимой основой для последующего изучения следующих дисциплин, указанных в пункте 7.1.

### 4. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу с обучающимися с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины «Информационная безопасность» в соответствии с рабочим учебным планом и ее распределение по видам работ представлены ниже.

#### Очная форма обучения

Семестр	Трудоемкость час/з.е.	Контактная работа с преподавателем, час			Самостоятельная работа, час	Контроль, час	Форма промежуточной аттестации (форма контроля)
		лекции	практические занятия	лабораторные занятия			
7	72/2	18	18	-	36	-	зачет
в т.ч. часов: в интерактивной форме		4	4	-	-	-	-
практической подготовки (при наличии)		18	18	-	36	-	-

Семестр	Трудоемкость час/з.е.	Внеаудиторная контактная работа с преподавателем, час/чел					
		Курсовая работа	Курсовой проект	Зачет	Дифференцированный зачет	Консультации перед экзаменом	Экзамен
7	72/2	-	-	0,12	-	-	-

#### Очно-заочная форма обучения

Семестр	Трудоемкость час/з.е.	Контактная работа с преподавателем, час			Самостоятельная работа, час	Контроль, час	Форма промежуточной аттестации (форма контроля)
		лекции	практические занятия	лабораторные занятия			
8	72/2	14	14	-	44	-	Зачет
в т.ч. часов: в интерактивной форме		2	4	-	-	-	-
практической подготовки (при наличии)		14	14	-	44	-	-

Семестр	Трудоемкость час/з.е.	Внеаудиторная контактная работа с преподавателем, час/чел						
		Контрольная работа	Курсовая работа	Курсовой проект	Зачет	Дифференцированный зачет	Консультации перед экзаменом	Экзамен
8	72/2	-	-	-	0,12	-	-	-

### 5. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

### Очная форма обучения

№ пп	Темы (и/или разделы) дисциплины	Количество часов					Формы текущего контроля успеваемости и промежуточной аттестации	Оценочное средство проверки результатов достижения индикаторов компетенций	Код индикаторов достижения компетенций
		Всего	Лекции	Семинарские занятия		Самостоятельная работа			
				Практические	Лабораторные				
1	Введение в дисциплину	8	2	2	-	4	опрос студентов; аудиторное выполнение практических заданий и оценка результатов их выполнения	письменный опрос, отчет о практическом занятии	ПК-1.1, ПК-1.2
2	Уязвимости и угрозы информационной безопасности.	8	2	2	-	4	опрос студентов; аудиторное выполнение практических заданий и оценка результатов их выполнения	письменный опрос, отчет о практическом занятии	ПК-1.1, ПК-1.2
3	Каналы утечки конфиденциальной информации.	8	2	2	-	4	опрос студентов; аудиторное выполнение практических заданий и оценка результатов их выполнения	письменный опрос, отчет о практическом занятии	ПК-1.1, ПК-1.2
4	Способы несанкционированного доступа к конфиденциальной информации.	8	2	2	-	4	опрос студентов; аудиторное выполнение практических заданий и оценка результатов их выполнения	письменный опрос, отчет о практическом занятии	ПК-1.1, ПК-1.2
5	Аутентификация и методы защиты информации.	8	2	2	-	4	опрос студентов; аудиторное выполнение практических заданий и оценка результатов их выполнения	письменный опрос, отчет о практическом занятии	ПК-1.1, ПК-1.2
6	Удаленные атаки в компьютерных сетях	8	2	2	-	4	опрос студентов; аудиторное выполнение практических заданий и оценка результатов их выполнения	письменный опрос, отчет о практическом занятии	ПК-1.1, ПК-1.2
7	Компьютерные вирусы и способы борьбы с ними	8	2	2	-	4	опрос студентов; аудиторное выполнение практических заданий и оценка результатов их выполнения	письменный опрос, отчет о практическом занятии	ПК-1.1, ПК-1.2

№ пп	Темы (и/или разделы) дисциплины	Количество часов					Формы текущего контроля успеваемости и промежуточной аттестации	Оценочное средство проверки результатов достижения индикаторов компетенций	Код индикаторов достижения компетенций
		Всего	Лекции	Семинарские занятия		Самостоятельная работа			
				Практические	Лабораторные				
8	Персонал как основная опасность утраты конфиденциальной информации	8	2	2	-	4	опрос студентов; аудиторное выполнение практических заданий и оценка результатов их выполнения	письменный опрос, отчет о практическом занятии	ПК-1.1, ПК-1.2
9	Политика информационной безопасности организации	8	2	2	-	4	опрос студентов; аудиторное выполнение практических заданий и оценка результатов их выполнения	письменный опрос, отчет о практическом занятии	ПК-1.1, ПК-1.2
Промежуточная аттестация		-	-	-	-	-	зачет		ПК-1.1, ПК-1.2
Практическая подготовка		72	18	18	-	36	-	-	
<b>Итого</b>		<b>72</b>	<b>18</b>	<b>18</b>	<b>-</b>	<b>36</b>			

#### Очно-заочная форма обучения

№ пп	Темы (и/или разделы) дисциплины	Количество часов					Формы текущего контроля успеваемости и промежуточной аттестации	Оценочное средство проверки результатов достижения индикаторов компетенций	Код индикаторов достижения компетенций
		Всего	Лекции	Семинарские занятия		Самостоятельная работа			
				Практические	Лабораторные				
1	Введение в дисциплину	6	2	-	-	4	аудиторное проведение лекции и оценка результатов усвоения учебного материала	тестирование по материалам лекции	ПК-1.1, ПК-1.2
2	Уязвимости и угрозы информационной безопасности.	6	2	-	-	4	аудиторное проведение лекции и оценка результатов усвоения учебного материала	тестирование по материалам лекции	ПК-1.1, ПК-1.2
3	Каналы утечки конфиденциальной информации.	10	2	2	-	6	аудиторное выполнение практических заданий и оценка результатов их выполнения	отчет о практическом занятии	ПК-1.1, ПК-1.2

№ пп	Темы (и/или разделы) дисциплины	Количество часов					Формы текущего контроля успеваемости и промежуточной аттестации	Оценочное средство проверки результатов достижения индикаторов компетенций	Код индикаторов достижения компетенций
		Всего	Лекции	Семинарские занятия		Самостоятельная работа			
				Практические	Лабораторные				
4	Способы несанкционированного доступа к конфиденциальной информации.	10	2	2	-	6	аудиторное выполнение практических заданий и оценка результатов их выполнения	отчет о практическом занятии	ПК-1.1, ПК-1.2
5	Аутентификация и методы защиты информации.	10	2	2	-	6	аудиторное выполнение практических заданий и оценка результатов их выполнения	отчет о практическом занятии	ПК-1.1, ПК-1.2
6	Удаленные атаки в компьютерных сетях	6	2	-	-	4	аудиторное проведение лекции и оценка результатов усвоения учебного материала	тестирование по материалам лекции	ПК-1.1, ПК-1.2
7	Компьютерные вирусы и способы борьбы с ними	6	-	2	-	4	аудиторное выполнение практических заданий и оценка результатов их выполнения	отчет о практическом занятии	ПК-1.1, ПК-1.2
8	Персонал как основная опасность утраты конфиденциальной информации	4	2	-	-	2	аудиторное проведение лекции и оценка результатов усвоения учебного материала	тестирование по материалам лекции	ПК-1.1, ПК-1.2
9	Политика информационной безопасности организации	6	-	2	-	4	аудиторное выполнение практических заданий и оценка результатов их выполнения	отчет о практическом занятии	ПК-1.1, ПК-1.2
<b>Промежуточная аттестация</b>		8	-	4	-	4	<b>контрольная работа</b>	результаты решения задач контрольной работы	ПК-1.1, ПК-1.2
							<b>зачет</b>		ПК-1.1, ПК-1.2
<i>Практическая подготовка</i>		72	14	14		44	-	-	
<b>Итого</b>		<b>72</b>	<b>14</b>	<b>14</b>	<b>-</b>	<b>44</b>	<b>-</b>	<b>-</b>	

**5.1. Лекционный курс с указанием видов интерактивной формы проведения занятий\***

Тема лекции (и/или наименование раздел) (вид интерактивной формы проведения занятий)/(практическая подготовка)	Содержание темы (и/или раздела)	Всего, часов / часов интерактивных занятий/ практическая подготовка		
		очная форма	заочная форма	очно-заочная форма
Тема 1. Введение в дисциплину (лекция дискуссия) (практическая подготовка)	Общая характеристика дисциплины «Информационная безопасность». Основные понятия и определения, используемые в дисциплине. Введение в информационную безопасность и защиту информации.	2/2/2		2/2/2
Тема 2. Уязвимости и угрозы информационной безопасности (практическая подготовка)	Виды представления информации в информационных системах и возможные каналы ее утечки. Уязвимости информации в информационных системах. Угрозы информационной безопасности информационных систем.	2/-/2		2/-/2
Тема 3. Способы несанкционированного доступа к конфиденциальной информации (проблемная лекция) (практическая подготовка)	Способы несанкционированного доступа к конфиденциальной информации в проводных информационных системах. Способы несанкционированного доступа к конфиденциальной информации в беспроводных информационных системах. Способы несанкционированного доступа к конфиденциальной информации в компьютерных системах и сетях	2/2/2		2/-/2
Тема 4. Каналы утечки конфиденциальной информации (практическая подготовка)	Понятие и классификация каналов утечки информации. Каналы утечки информации в информационных системах.	2/-/2		2/-/2
Тема 5. Аутентификация и методы защиты информации (практическая подготовка)	Понятие и классификация глобальных информационных сетей. Технологии глобальных информационных сетей. Основные сервисы глобальных информационных сетей.	2/-/2		2/-/2
Тема 6. Удаленные атаки в компьютерных сетях (практическая подготовка)	Классификация атак в компьютерных сетях. Способы защиты информации в компьютерных сетях.	2/-/2		2/-/2
Тема 7. Компьютерные вирусы и способы борьбы с ними (практическая подготовка)	Компьютерные вирусы и их классификация. Жизненный цикл компьютерных вирусов и способы их распространения. Методы защиты от компьютерных вирусов и анти-вирусные программы.	2/-/2		-/-/-
Тема 8. Персонал как основная опасность утраты конфиденциальной информации (практическая подготовка)	Роль человеческого фактора в обеспечении безопасности информации. Методы добывания ценной информации у персонала.	2/-/2		2/-/2

Тема 9. Политика информационной безопасности организации (практическая подготовка)	Основы обеспечения режима информационной безопасности на предприятии. Основы анализа информационных рисков компании. Формирование политики информационной безопасности на предприятии.	2/-/2		-/-/-
<b>Итого</b>	-	<b>18/4/18</b>		<b>14/2/14</b>

**5.2. Семинарские (практические, лабораторные) занятия с указанием видов проведения занятий в интерактивной форме\***

Наименование раздела дисциплины	Формы проведения и темы занятий (вид интерактивной формы проведения занятий)/(практическая подготовка)	Всего часов / часов интерактивных занятий/ практическая подготовка					
		очная форма		заочная форма		очно-заочная форма	
		прак	лаб	прак	лаб	прак	лаб
Тема 1. Введение в дисциплину	<u>Практическое занятие</u> Защита от копирования данных съемных носителей (практическая подготовка)	2/-/2	-		-	-/-/-	-
Тема 2. Уязвимости и угрозы информационной безопасности	<u>Практическое занятие</u> Изучение уязвимостей Windows (практическая подготовка)	2/-/2	-		-	-/-/-	-
Тема 3. Способы несанкционированного доступа к конфиденциальной информации	<u>Практическое занятие</u> Исследование способов удаления и восстановления компьютерной информации (творческое задание) (практическая подготовка)	2/2/2	-			2/2/2	
Тема 4. Каналы утечки конфиденциальной информации	<u>Практическое занятие</u> Защита автоматизированной системы обработки конфиденциальной информации от побочного электромагнитного излучения и наводок (практическая подготовка)	2/-/2	-		-	2/-/2	-
Тема 5. Аутентификация и методы защиты информации	<u>Практическое занятие</u> Изучение аппаратных ключей защиты (практическая подготовка)	2/-/2	-			2/-/2	
Тема 6. Удаленные атаки в компьютерных сетях	<u>Практическое занятие</u> Изучение компьютерных вирусов (практическая подготовка)	2/-/2	-		-	-/-/-	-
Тема 7. Компьютерные вирусы и способы борьбы с ними	<u>Практическое занятие</u> Изучение антивирусного программного обеспечения (творческое задание) (практическая подготовка)	2/2/2	-			2/2/2	
Тема 8. Персонал	<u>Практическое занятие</u> Изуче-	2/-/2	-		-	-/-/-	-



как основная опасность утраты конфиденциальной информации	ние назначения и областей применения электронной подписи ( <i>практическая подготовка</i> )						
Тема 9. Политика информационной безопасности организации	<u>Практическое занятие</u> Изучение генераторов паролей ( <i>практическая подготовка</i> )	2/-/2	-			2/-/2	
	Контрольная работа (аудиторная) ( <i>практическая подготовка</i> )	-	-		-	4/-/4	-
<b>Итого</b>		<b>18/4/18</b>	-		-	<b>14/4/14</b>	-

Интерактивные формы проведения занятий, предусмотренные рабочей программой дисциплины, проводятся в соответствии с Положением об интерактивных формах обучения в ФГБОУ ВО Ставропольский ГАУ.

### 5.3. Курсовой проект (работа) учебным планом не предусмотрен.

### 5.4. Самостоятельная работа обучающегося

Виды самостоятельной работы	Очная форма, часов		Заочная форма, часов		Очно-заочная форма, часов	
	к текущему контролю	к промежуточной аттестации	к текущему контролю	к промежуточной аттестации	к текущему контролю	к промежуточной аттестации
<b>Подготовка к практическим занятиям:</b>						
подготовка к опросам	10	-	-	-	8	-
подготовка и выполнение практических задач и отчетов в рабочей тетради	20	-	-	-	22	-
подготовка творческого задания	2	-	-	-	2	-
подготовка эссе, доклада, статьи	2	-	-	-	2	-
подготовка к контрольным точкам	2	-	-	-	10	-
подготовка к контрольной работе (аудиторной)	-	-	-	-	-	-
<b>ИТОГО</b>	<b>36</b>	-	-	-	<b>44</b>	-

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

Учебно-методическое обеспечение для самостоятельной работы обучающегося по дисциплине «Информационная безопасность» размещено в электронной информационно-образовательной среде Университета и доступно для обучающегося через его личный кабинет на сайте Университета. Учебно-методическое обеспечение включает:

1. Рабочую программу дисциплины «Информационная безопасность».
2. Методические рекомендации по освоению дисциплины «Информационная безопасность».
3. Методические рекомендации для организации самостоятельной работы обучающегося по дисциплине «Информационная безопасность».

Для успешного освоения дисциплины, необходимо самостоятельно детально изучить представленные темы по рекомендуемым источникам информации:

№ п/п	Темы для самостоятельного изучения	Рекомендуемые источники информации (№ источника)		
		основная (из п.8 РПД)	дополни- тельная (из п.8 РПД)	интернет- ресурсы (из п.9 РПД)
1	Классификация уровней защищенности персональных данных	1,2,3,4	5	1,2,3,4
2	Мероприятия по организационному обеспечению безопасности персональных данных	1,2	5	1,2
3	Общий порядок организации обеспечения безопасности персональных данных в информационных системах персональных данных (ИСПДн)	3,4	5	1,2
4	Пассивные и активные методы, используемые для создания системы защиты персональных данных	3,4	5	1,2,3,4
5	Средства защиты информации экономических информационных систем	3,4	5	1,2,3,4
6	Сертификация средств защиты информации	1,2	5	3,4
7	Лицензирование деятельности по защите конфиденциальной информации	1,2,3,4	5	1,2,3,4
8	Аттестация объектов информатизации по требованиям безопасности информации	1,2,3,4	5	1,2,3,4
9	Организация и обеспечение безопасности информации с использованием шифровальных (криптографических) средств	1,2,3,4	5	1,2,3,4



Индикатор компетенции (код и содержание)	Дисциплины/элементы программы (практики, ГИА), участвующие в формировании индикатора компетенции	Семестры									
		1	2	3	4	5	6	7	8	9	10
	ства										
	Механизация сельскохозяйственного производства										
	Технология производства, переработки и хранения продукции растениеводства										
	Международная торговля										
ПК-2.1 Обосновывает и применяет статистические, экономико-математические, маркетинговые методы исследования внешней среды и деятельности организации, проводит расчеты финансово-экономических показателей, в т.ч. с использованием типовых методик и нормативно-правовых актов.	Статистика										
	Общая теория статистики										
	Социально-экономическая статистика										
	Методы оптимальных решений										
	Экономический анализ										
	Экономический практикум										
	Моделирование бизнес-процессов предприятия в среде 1С										
	Маркетинг										
	Планирование деятельности организации										
	Антимонопольная политика и защита прав потребителей										
	Правовое обеспечение финансово-хозяйственной деятельности организации										
	Технологии продвижения продукции (услуг)										
	Внешнеэкономическая деятельность организации										
	Маркетинговые исследования										
	Экономика отраслевых рынков										
	Ценообразование										
	Системы электронного документооборота										
	Информационная безопасность								+		
	Технологическая (проектно-технологическая) практика										
	Преддипломная практика										
Подготовка к сдаче и сдача государственного экзамена											





Индикатор компетенции (код и содержание)	Дисциплины/элементы программы (практики, ГИА), участвующие в формировании индикатора компетенции	Семестры									
		1	2	3	4	5	6	7	8	9	10
	Информационная безопасность								+		
	Технологическая (проектно-технологическая) практика										
	Преддипломная практика										
	Подготовка к сдаче и сдача государственного экзамена										
	Подготовка к процедуре защиты и защита выпускной квалификационной работы										
	Практикум по интернет-маркетингу										
	Анализ, совершенствование и управление бизнес-процессами										

## 7.2. Критерии и шкалы оценивания уровня усвоения индикатора компетенций, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Оценка знаний, умений и навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций по дисциплине «Информационная безопасность» проводится в форме текущего контроля и промежуточной аттестации.

Текущий контроль проводится в течение семестра с целью определения уровня усвоения обучающимися знаний, формирования умений и навыков, своевременного выявления преподавателем недостатков в подготовке обучающихся и принятия необходимых мер по её корректировке, а также для совершенствования методики обучения, организации учебной работы и оказания индивидуальной помощи обучающемуся.

Промежуточная аттестация по дисциплине «Информационная безопасность» проводится в виде зачета.

За знания, умения и навыки, приобретенные студентами в период их обучения, выставляются оценки «ЗАЧТЕНО», «НЕ ЗАЧТЕНО».

Для оценивания знаний, умений, навыков и (или) опыта деятельности в университете применяется балльно-рейтинговая система оценки качества освоения образовательной программы. Оценка проводится при проведении текущего контроля успеваемости и промежуточных аттестаций обучающихся. Рейтинговая оценка знаний является интегрированным показателем качества теоретических и практических знаний и навыков студентов по дисциплине.

### Состав балльно-рейтинговой оценки студентов очной формы обучения

Для студентов очной формы обучения знания по осваиваемым компетенциям формируются на лекционных и практических занятиях, а также в процессе самостоятельной подготовки.

В соответствии с балльно-рейтинговой системой оценки, принятой в Университете студентам начисляются баллы по следующим видам работ:

№ контрольной точки	Оценочное средство результатов индикаторов достижения компетенций***	Максимальное количество баллов
1.	Опрос студентов; аудиторное выполнение практических заданий и оценка результатов их выполнения	3

№ контрольной точки	Оценочное средство результатов индикаторов достижения компетенций***	Максимальное количество баллов
	Выполнение тестовых заданий по теме №1	4
2.	Опрос студентов; аудиторное выполнение практических заданий и оценка результатов их выполнения	3
	Выполнение тестовых заданий по теме №2	4
3.	Опрос студентов; аудиторное выполнение практических заданий и оценка результатов их выполнения	3
	Выполнение тестовых заданий по теме №3	4
4.	Опрос студентов; аудиторное выполнение практических заданий и оценка результатов их выполнения по теме №4	3
	Выполнение тестовых заданий	4
5.	Опрос студентов; аудиторное выполнение практических заданий и оценка результатов их выполнения по теме №5	3
	Выполнение тестовых заданий	4
6.	Опрос студентов; аудиторное выполнение практических заданий и оценка результатов их выполнения по теме №6	3
	Выполнение тестовых заданий	4
7.	Опрос студентов; аудиторное выполнение практических заданий и оценка результатов их выполнения по теме №7	3
	Выполнение тестовых заданий	3
8.	Опрос студентов; аудиторное выполнение практических заданий и оценка результатов их выполнения по теме №8	3
	Выполнение тестовых заданий	3
9.	Опрос студентов; аудиторное выполнение практических заданий и оценка результатов их выполнения по теме №9	3
	Выполнение тестовых заданий	3
<b>Сумма баллов по итогам текущего контроля</b>		<b>60</b>
Активность на лекционных занятиях		10
Результативность работы на практических занятиях		15
Поощрительные баллы (написание статей, участие в конкурсах, олимпиадах, выступления на конференциях, и т.д.)		15
<b>Итого</b>		<b>100</b>

\*\*\* Оценочное средство результатов индикаторов достижения компетенций – совпадает с теми, что даны в п. 5.1.

### Критерии и шкалы оценивания уровня усвоения индикатора компетенций

Знания по осваиваемым компетенциям формируются **на лекционных занятиях** при условии активного участия, обучающегося в восприятии и обсуждении рассматриваемых вопросов.

#### Критерии и шкала оценки посещения и активности на лекционных занятиях

Процент посещения и активности на лекционных занятиях	Начисляемые баллы				Максимальный начисленный балл за семестр
	I	II	III	IV	
до 50%	2 балла	2 балла	1 балл	1 балла	6 баллов
свыше 50%	3 балла	3 балла	2 балла	2 балла	10 баллов

#### Результативность работы на практических занятиях

##### Выполнение практических задач

Выполнение практических задач на практических занятиях является одной из основных форм оценивания компетенций студентов. С помощью предложенных компьютерных средств решения практиче-



ских задач студент должен получить и предоставить на проверку отчет о практическом занятии и выполненное задание.

### ***Выполнение заданий рабочей тетради***

Рабочая тетрадь – дидактический комплекс, предназначен для организации аудиторной и самостоятельной работы обучающихся при изучении дисциплины «Информационная безопасность». Материал рабочей тетради расположен по темам в соответствии с учебно-тематическим планом курса.

Необходимость использования обучающимися рабочей тетради состоит в: закреплении теоретических знаний, полученных в процессе лекций; получении практических навыков в решении задач и проблемных ситуаций; самостоятельном овладении дополнительным материалом курса.

Рабочая тетрадь позволяет адекватно оценить знания и навыки обучающихся на любом этапе учебного процесса при условии своевременного изучения источников и литературы по программе курса, использовании лекционного материала и самостоятельной работы.

Особенностью рабочей тетради является ее накопительный характер, позволяющий в конце каждой темы провести работу по систематизации освоенного материала, повторной проработки, рефлексии и т.д.

### **Критерии и шкала оценки выполнения практических задач и заданий рабочей тетради (максимум 4,5)**

4,5 баллов – за оцененное на «отлично» выполнение заданий практических занятий и рабочей тетради по каждой из тем;

3 балла – за оцененное на «хорошо» выполнение заданий практических занятий и рабочей тетради по каждой из тем;

1,5 балла – за оцененное на «удовлетворительно» выполнение заданий практических занятий и рабочей тетради по каждой из тем.

***Письменный опрос*** - средство контроля, организованное как письменный ответ на поставленные вопросы обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний, обучающегося по определенному разделу, теме, проблеме и т.п.

### **Критерии и шкала оценки письменного ответа (максимум 1,5 балла)**

**1,5 балла** если обучающийся строит ответ логично, показывает максимально глубокие знания профессиональных терминов, понятий, категорий, концепций и теорий. Развернуто аргументирует выдвигаемые положения, приводит убедительные примеры. Обнаруживает способность анализа в освещении различных концепций. Делает содержательные выводы. Демонстрирует знание специальной литературы в рамках учебного методического комплекса и дополнительных источников информации;

**1 балл** если обучающийся строит ответ логично, показывает максимально глубокие знания профессиональных терминов, понятий, категорий, концепций и теорий. Развернуто аргументирует выдвигаемые положения, приводит убедительные примеры. Демонстрирует знание специальной литературы в рамках учебного методического комплекса и дополнительных источников информации;

**0,5 балла** если ответ недостаточно логически выстроен, обучающийся обнаруживает слабость в развернутом раскрытии профессиональных понятий. Выдвигаемые положения декларируются, но недостаточно аргументированы. Ответ носит преимущественно теоретический характер, примеры ограничены, либо отсутствуют;

**0 баллов** при условии недостаточного раскрытия профессиональных понятий, категорий, концепций, теорий. Обучающийся проявляет стремление подменить научное обоснование проблем рассуждениями обыденно-повседневного бытового характера. Ответ содержит ряд серьезных неточностей. Выводы поверхностны.

***Доклад*** – продукт самостоятельной работы студента, представляющий собой публичное выступление по представлению полученных результатов решения определенной учебно-практической темы.

### **Критерии и шкала оценки доклада (1 балл)**

**1 балл.** Выступление демонстрирует умения умение правильно использовать в устной речи специальные термины и понятия, показатели; синтезировать, анализировать, обобщать представленный материал, устанавливать причинно-следственные связи, формулировать правильные выводы; аргументировать собственную точку зрения, активно использовать самостоятельно подготовленную презентацию.

**0,8 балла.** В выступлении отсутствует обобщение представленного материала, установлены не все причинно-следственные связи.

**0,6 балла.** В выступлении отсутствует обобщение представленного материала, установлены не все причинно-следственные связи, обучающийся не всегда правильно использует в устной речи специальные термины и понятия, показатели, допущены ошибки в самостоятельно подготовленной презентации.

**0 баллов** - выставляется обучающемуся, если доклад, обучающимся не представлен.

*Эссе* - средство, позволяющее оценить умение обучающегося письменно излагать суть поставленной проблемы, самостоятельно проводить анализ этой проблемы с использованием концепций и аналитического инструментария дисциплины, делать выводы, обобщающие авторскую позицию по поставленной проблеме.

#### **Критерии и шкала оценки эссе (максимум 1 балл)**

**1 балл** - выставляется обучающемуся, если эссе включает в себя следующие параметры, каждый из которых несет собственную высокую ценность: определение предмета эссе; обозначение круга научных понятий и теорий, понимание и правильное использование специальных терминов; использование основных категорий анализа, выделение причинно-следственных связей; применение аппарата сравнительных характеристик; сохранение логики рассуждений при переходе от одной части к другой; аргументация основных положений эссе; умение делать промежуточные и конечные выводы; иллюстрация научных понятий соответствующими практическими примерами; способность дать личную субъективную оценку по исследуемой проблеме; презентация эссе, включающая умение разделить эссе на смысловые части;

**0,8 балла** - выставляется обучающемуся, если основные требования к эссе и его оформлению, но при этом допущены недочеты. В частности, имеются неточности в использовании специальных терминов; отсутствует логическая последовательность в суждениях; не выдержана структура презентации эссе; на дополнительные вопросы при презентации эссе даны неполные ответы;

**0,6 балла** - выставляется обучающемуся, если имеются существенные отступления от требований к написанию эссе. В частности, тема освещена лишь частично; нарушена логика рассуждений при переходе от одной части к другой; недостаточно представлена аргументация основных положений эссе;

**0 баллов** - выставляется обучающемуся, если тема эссе не раскрыта, обнаруживается существенное непонимание проблемы, либо эссе, обучающимся не представлено.

#### **Занятия, проводимые в интерактивной форме**

*Творческое задание* - частично регламентированное задание, имеющее нестандартное решение и позволяющее диагностировать умения, интегрировать знания различных областей, аргументировать собственную точку зрения; может выполняться в индивидуальном порядке или группой обучающихся из 2-3 человек

#### **Критерии и шкала оценки выполнения творческого задания (максимум 7 баллов)**

**7 баллов** выставляется обучающемуся, если материал изложен грамотно, доступно, логично и интересно; стиль изложения соответствует задаче творческого задания; задание выполнено на высоком профессиональном уровне; представленный материал фактически верен; обучающийся свободно отвечает на вопросы, связанные с творческим заданием;

**5 баллов** выставляется обучающемуся, если задание выполнено на достаточно высоком профессиональном уровне; допущены отдельные фактические ошибки, логические и стилистические погрешности; обучающийся отвечает на вопросы, связанные с творческим заданием, но недостаточно полно;

**3 балла** выставляется обучающемуся, если уровень изложения материала по результатам выполнения творческого задания недостаточно высок; допущено незначительное количество фактических ошибок в расчетах; обучающийся может ответить, лишь на некоторые вопросы, относящиеся к творческому заданию;

**1 балл** выставляется обучающемуся, если творческое задание выполнено на низком уровне; допущено существенное количество ошибок в расчетах; неясность и примитивность изложения результаты выполнения творческого задания трудными для восприятия; обучающийся затрудняется ответить, на большее количество вопросов, относящихся к творческому заданию.

Рейтинговая оценка знаний при проведении текущего контроля успеваемости **на контрольных точках** позволяет обучающемуся набрать до 60 баллов. Знания, умения и навыки по формируемым компетенциям оцениваются по результатам следующих форм контроля.

*Тестирование* - система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний, умений, навыков обучающегося.

**Критерии и шкала оценки контрольных точек (тестирование). Каждая контрольная точка - мах 12 баллов)**

**10-12 баллов** выставляется обучающемуся, если тестовые задания выполняются на 85% и выше;

**7-9 баллов** выставляется обучающемуся, если тестовые задания выполняются на 70 - 84%;

**4-6 баллов** выставляется обучающемуся, если тестовые задания выполняются на 55 – 69 %;

**1-3 балла** выставляется обучающемуся, если тестовые задания выполняются на 45 – 54%;

**0 баллов** выставляется обучающемуся, если тестовые задания выполняются на 44% и меньше.

Если за письменные ответы на контрольной точке обучающийся не получил удовлетворяющее его количество баллов, то он может получить **поощрительные баллы за подготовку статей, выступление на конференции, участие в конкурсах (не более 15 баллов)**.

**Статья** – средство, позволяющее оценить умение обучающегося письменно излагать суть поставленной проблемы, самостоятельно проводить ее анализ с использованием знаний, умений и навыков, приобретаемых в рамках изучения предыдущих и данной дисциплины, делать выводы, обобщающие авторскую позицию по поставленной проблеме.

**Критерии и шкала оценки научной статьи (мах 15 баллов)**

**15 баллов.** Статья объемом не менее 4 страниц демонстрирует умение проведения самостоятельного актуального научно-практического исследования, правильно оформлена, содержит оригинальный анализ проблемы, подтвержденный статистическими и/или отчетными данными, графическим материалом. В ней рассмотрены возможные пути решения проблемы, сформулировать правильные выводы и предложения, отражающие авторскую точку зрения.

**10 баллов.** Статья объемом не менее 3 страниц демонстрирует умение проведения самостоятельного актуального научно-практического исследования, правильно оформлена, содержит типовой анализ проблемы, подтвержденный статистическими и/или отчетными данными. В ней рассмотрены возможные пути решения проблемы, сформулировать правильные выводы и предложения.

**5 баллов.** Статья объемом не менее 2 страниц представлена в виде тезисов, демонстрирует умение проведения самостоятельного актуального научно-практического исследования, правильно оформлена, содержит анализ проблемы, подтвержденный отдельными статистическими и/или отчетными данными. В ней сформулированы правильные выводы и предложения.

### **Состав балльно-рейтинговой оценки студентов заочной формы обучения**

Для студентов **очно-заочной формы обучения** знания по осваиваемым компетенциям формируются на **лекционных и практических занятиях, а также в процессе самостоятельной подготовки**.

Результат текущего контроля для обучающихся **очно-заочной формы обучения** складывается из оценки результатов обучения по всем разделам дисциплины и включает (**мах 10 баллов**), оценку результативности работы на практических и семинарских занятиях: а) письменный опрос, решение практических заданий (**мах 8 баллов**); б) активное участие в занятиях, проводимых в интерактивной форме, подготовка творческих заданий (**мах 7 баллов**), оценку контрольных точек: подготовка и выполнение практических задач и заданий в рабочей тетради (**мах 30 баллов**) и контрольную точку в виде контрольной работы (аудиторной) - тестирования по всем разделам дисциплины (**мах 30 баллов**), поощрительные баллы (**мах 15 баллов**).

В соответствии с балльно-рейтинговой системой оценки, принятой в Университете студентам начисляются баллы по следующим видам работ:

<b>№ контрольной точки</b>	<b>Оценочное средство результатов индикаторов достижения компетенций</b>	<b>Максимальное количество баллов</b>
1.	Подготовка и выполнение практических задач и заданий в рабочей тетради	30
2.	Контрольная работа по всем темам дисциплины (аудиторная) - тестирование	30
<b>Сумма баллов по итогам текущего контроля</b>		60
Активность на лекционных занятиях		10
Результативность работы на практических занятиях (активное участие в занятиях, подготовка творческих заданий и пр.)		15

№ контрольной точки	Оценочное средство результатов индикаторов достижения компетенций	Максимальное количество баллов
	Поощрительные баллы (написание статей, участие в конкурсах, на олимпиадах, выступления на конференциях и т.д.)	15
	Итого	100

Оценочное средство результатов достижения компетенций – совпадает с теми, что даны в п. 5.1.

### Критерии и шкалы оценивания уровня усвоения индикатора компетенций

Знания по осваиваемым компетенциям формируются на лекционных занятиях при условии активного участия, обучающегося в восприятии и обсуждении рассматриваемых вопросов.

#### Критерии и шкала оценки посещения и активности на лекционных занятиях

Процент посещения и активности на лекционных занятиях	Максимально начисленный балл
до 50%	6 баллов
свыше 50%	10 баллов

### Результативность работы на практических занятиях

#### *Выполнение практических задач*

Выполнение практических задач на практических занятиях является одной из основных форм оценивания компетенций студентов. С помощью предложенных компьютерных средств решения практических задач студент должен получить и предоставить на проверку отчет о практическом занятии и выполненное задание.

#### *Выполнение заданий рабочей тетради*

Рабочая тетрадь – дидактический комплекс, предназначен для организации аудиторной и самостоятельной работы обучающихся при изучении дисциплины «Информационная безопасность». Материал рабочей тетради расположен по темам в соответствии с учебно-тематическим планом курса.

Необходимость использования обучающимися рабочей тетради состоит в: закреплении теоретических знаний, полученных в процессе лекций; получении практических навыков в решении задач и проблемных ситуаций; самостоятельном овладении дополнительным материалом курса.

Рабочая тетрадь позволяет адекватно оценить знания и навыки обучающихся на любом этапе учебного процесса при условии своевременного изучения источников и литературы по программе курса, использовании лекционного материала и самостоятельной работы.

Особенностью рабочей тетради является ее накопительный характер, позволяющий в конце каждой темы провести работу по систематизации освоенного материала, повторной проработки, рефлексии и т.д.

#### **Критерии и шкала оценки выполнения практических задач и заданий рабочей тетради (максимум 30 баллов)**

30 баллов – за оцененное на «отлично» выполнение практических задач и заданий рабочей тетради по каждой из тем, выносимых на практические занятия;

20 баллов – за оцененное на «хорошо» выполнение практических задач и заданий рабочей тетради по каждой из тем, выносимых на практические занятия;

10 баллов – за оцененное на «удовлетворительно» выполнение практических задач и заданий рабочей тетради по каждой из тем, выносимых на практические занятия.

**Письменный опрос** - средство контроля, организованное как письменный ответ на поставленные вопросы обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний, обучающегося по определенному разделу, теме, проблеме и т.п.

#### **Критерии и шкала оценки письменного ответа (максимум 2 балла)**

**2 балла** если обучающийся строит ответ логично, показывает максимально глубокие знания профессиональных терминов, понятий, категорий, концепций и теорий. Развернуто аргументирует выдвигаемые положения, приводит убедительные примеры. Обнаруживает способность анализа в освеще-

нии различных концепций. Делает содержательные выводы. Демонстрирует знание специальной литературы в рамках учебного методического комплекса и дополнительных источников информации;

**1,5 балла** если обучающийся строит ответ логично, показывает максимально глубокие знания профессиональных терминов, понятий, категорий, концепций и теорий. Развернуто аргументирует выдвигаемые положения, приводит убедительные примеры. Демонстрирует знание специальной литературы в рамках учебного методического комплекса и дополнительных источников информации;

**1 балл** если ответ недостаточно логически выстроен, обучающийся обнаруживает слабость в развернутом раскрытии профессиональных понятий. Выдвигаемые положения декларируются, но недостаточно аргументированы. Ответ носит преимущественно теоретический характер, примеры ограничены, либо отсутствуют;

**0 баллов** при условии недостаточного раскрытия профессиональных понятий, категорий, концепций, теорий. Обучающийся проявляет стремление подменить научное обоснование проблем рассуждениями обыденно-повседневного бытового характера. Ответ содержит ряд серьезных неточностей. Выводы поверхностны.

### **Занятия, проводимые в интерактивной форме**

**Творческое задание** - частично регламентированное задание, имеющее нестандартное решение и позволяющее диагностировать умения, интегрировать знания различных областей, аргументировать собственную точку зрения; может выполняться в индивидуальном порядке или группой обучающихся из 2-3 человек

#### **Критерии и шкала оценки выполнения творческого задания (максимум 7 баллов)**

**7 баллов** выставляется обучающемуся, если материал изложен грамотно, доступно, логично и интересно; стиль изложения соответствует задаче творческого задания; задание выполнено на высоком профессиональном уровне; представленный материал фактически верен; обучающийся свободно отвечает на вопросы, связанные с творческим заданием;

**5 баллов** выставляется обучающемуся, если задание выполнено на достаточно высоком профессиональном уровне; допущены отдельные фактические ошибки, логические и стилистические погрешности; обучающийся отвечает на вопросы, связанные с творческим заданием, но недостаточно полно;

**3 балла** выставляется обучающемуся, если уровень изложения материала по результатам выполнения творческого задания недостаточно высок; допущено незначительное количество фактических ошибок в расчетах; обучающийся может ответить, лишь на некоторые вопросы, относящиеся к творческому заданию;

**1 балл** выставляется обучающемуся, если творческое задание выполнено на низком уровне; допущено существенное количество ошибок в расчетах; неясность и примитивность изложения результаты выполнения творческого задания трудными для восприятия; обучающийся затрудняется ответить, на большее количество вопросов, относящихся к творческому заданию.

Рейтинговая оценка знаний при проведении текущего контроля успеваемости студентов **очно-заочной формы** обучения на контрольных точках позволяет обучающемуся набрать до 60 баллов. Знания, умения и навыки по формируемым компетенциям оцениваются по результатам следующих форм контроля.

**Эссе** - средство, позволяющее оценить умение обучающегося письменно излагать суть поставленной проблемы, самостоятельно проводить анализ этой проблемы с использованием концепций и аналитического инструментария дисциплины, делать выводы, обобщающие авторскую позицию по поставленной проблеме.

#### **Критерии и шкала оценки эссе (максимум 1 балл)**

**1 балл** - выставляется обучающемуся, если эссе включает в себя следующие параметры, каждый из которых несет собственную высокую ценность: определение предмета эссе; обозначение круга научных понятий и теорий, понимание и правильное использование специальных терминов; использование основных категорий анализа, выделение причинно-следственных связей; применение аппарата сравнительных характеристик; сохранение логики рассуждений при переходе от одной части к другой; аргументация основных положений эссе; умение делать промежуточные и конечные выводы; иллюстрация научных понятий соответствующими практическими примерами; способность дать личную субъективную оценку по исследуемой проблеме; презентация эссе, включающая умение разделить эссе на смысловые части;

**0,8 балла** - выставляется обучающемуся если основные требования к эссе и его оформлению, но при этом допущены недочёты. В частности, имеются неточности в использовании специальных терминов; отсутствует логическая последовательность в суждениях; не выдержана структура презентации эссе; на дополнительные вопросы при презентации эссе даны неполные ответы;

**0,6 балла** - выставляется обучающемуся, если имеются существенные отступления от требований к написанию эссе. В частности, тема освещена лишь частично; нарушена логики рассуждений при переходе от одной части к другой; недостаточно представлена аргументация основных положений эссе;

**0 баллов** - выставляется обучающемуся, если тема эссе не раскрыта, обнаруживается существенное непонимание проблемы, либо эссе, обучающимся не представлено.

**Контрольная работа (аудиторная) - тестирование** - система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний, умений, навыков обучающегося.

**Критерии и шкала оценки контрольной точки по всем темам дисциплины (аудиторная) - тестирование (максимум 30 баллов)**

**25-30 баллов** выставляется обучающемуся, если тестовые задания выполняются на 85% и выше;

**15-24 баллов** выставляется обучающемуся, если тестовые задания выполняются на 70 - 84%;

**10-14 баллов** выставляется обучающемуся, если тестовые задания выполняются на 55 - 69 %;

**1-9 баллов** выставляется обучающемуся, если тестовые задания выполняются на 45 - 54%;

**0 баллов** выставляется обучающемуся, если тестовые задания выполняются на 44% и меньше.

Если за письменные ответы на контрольной точке обучающийся не получил удовлетворяющее его количество баллов, то он может получить **поощрительные баллы за подготовку статей, выступление на конференции, участие в конкурсах (не более 15 баллов)**.

**Статья** – средство, позволяющее оценить умение обучающегося письменно излагать суть поставленной проблемы, самостоятельно проводить ее анализ с использованием знаний, умений и навыков, приобретаемых в рамках изучения предыдущих и данной дисциплины, делать выводы, обобщающие авторскую позицию по поставленной проблеме.

**Критерии и шкала оценки научной статьи (максимум 15 баллов)**

**15 баллов.** Статья объемом не менее 4 страниц демонстрирует умение проведения самостоятельного актуального научно-практического исследования, правильно оформлена, содержит оригинальный анализ проблемы, подтвержденный статистическими и/или отчетными данными, графическим материалом. В ней рассмотрены возможные пути решения проблемы, сформулировать правильные выводы и предложения, отражающие авторскую точку зрения.

**10 баллов.** Статья объемом не менее 3 страниц демонстрирует умение проведения самостоятельного актуального научно-практического исследования, правильно оформлена, содержит типовой анализ проблемы, подтвержденный статистическими и/или отчетными данными. В ней рассмотрены возможные пути решения проблемы, сформулировать правильные выводы и предложения.

**5 баллов.** Статья объемом не менее 2 страниц представлена в виде тезисов, демонстрирует умение проведения самостоятельного актуального научно-практического исследования, правильно оформлена, содержит анализ проблемы, подтвержденный отдельными статистическими и/или отчетными данными. В ней сформулированы правильные выводы и предложения.

При проведении итоговой аттестации «зачет» преподавателю с согласия студента разрешается выставлять оценку «зачет» по результатам набранных баллов в ходе текущего контроля успеваемости в семестре по выше приведенной шкале.

В случае отказа – студент сдает зачет по приведенным выше вопросам и заданиям. Итоговая успеваемость *зачет* не может оцениваться ниже суммы баллов, которую студент набрал по итогам текущей и промежуточной успеваемости.

При сдаче *зачета* к заработанным в течение семестра студентом баллам прибавляются баллы, полученные на *зачете* и сумма баллов переводится в оценку.

### **Критерии и шкалы оценивания ответа на зачете**

По дисциплине «Информационная безопасность» к зачету допускаются студенты, выполнившие и сдавшие практические работы по дисциплине, имеющие ежемесячную аттестацию и наличие по текущей успеваемости более 45 баллов. Студентам, набравшим более 55 баллов, зачет выставляется по результатам текущей успеваемости, студенты, набравшие от 45 до 54 баллов, сдают зачет по вопросам, предусмотренным РПД.

### **7.3. Примерные оценочные материалы для текущего контроля успеваемости и промежуточной аттестации по итогам освоения дисциплины «Информационная безопасность»**

#### **Вопросы для письменного опроса по дисциплине «Информационная безопасность» (фрагмент)**

1. Дайте определение и охарактеризуйте процедуры идентификации и аутентификации.
2. Охарактеризуйте методы аутентификации, используемые в телекоммуникационных системах.
3. Дайте общую характеристику методам защиты от электромагнитных излучений.
4. Поясните сущность экранирования в телекоммуникационных системах.
5. Поясните сущность снижения мощности электромагнитных излучений и наводок в телекоммуникационных системах.
6. Поясните сущность способов заземления и особенностей их применения в телекоммуникационных системах.
7. Поясните сущность фильтрации опасных сигналов в телекоммуникационных системах.
8. Охарактеризуйте активные методы защиты информации в телекоммуникационных системах.

#### **Практические задания для оценки компетенций студентов по дисциплине «Информационная безопасность» (фрагмент)**

##### **Задача 1.**

1. Ознакомиться с описанием лабораторной работы и заданием.
2. Для одноалфавитного метода с фиксированным смещением определить установленное в программе смещение. Для этого следует:
  - просмотреть предварительно созданный с помощью редактора свой текстовый файл;
  - выполнить для этого файла шифрование;
  - просмотреть в редакторе зашифрованный файл;
  - просмотреть гистограммы исходного и зашифрованного текстов;
  - описать гистограммы (в чем похожи, в чем отличаются) и определить, с каким смещением было выполнено шифрование;
  - расшифровать зашифрованный текст:
    - 1) С помощью гистограммы, после чего проверить в редакторе правильность расшифрования;
    - 2) Вручную с помощью гистограмм, описать и объяснить процесс дешифрования.

В отчете для каждого метода шифрования описывается последовательность выполняемых действий, имена всех использованных файлов, полученные гистограммы, указывается найденное смещение, описывается процесс дешифрования.

Преподавателю предоставляется отчет о проделанной работе и все использованные и созданные файлы.

##### **Задача 2.**

Запустить программу, предназначенную для демонстрации порядка постановки и проверки электронной подписи.

Сгенерировать и переслать участникам обмена ключи для шифрования исходного документа и ключи для подписания документа. Исходный текст для шифрования набирается непосредственно в окне программы.

Зашифровать исходное сообщение и подписать его на секретном ключе отправителя.

Переслать зашифрованное и подписанное сообщение получателю. Выполнить проверку правильности ЭП и восстановить исходный текст сообщения.

Сохранить в отчете экранные формы, демонстрирующие процесс генерации и распространения ключей; процесс шифрования исходного документа и постановки ЭП.

Привести в отчете ответы на контрольные вопросы, в соответствии с номером варианта, указанным преподавателем.

Оформите отчет о выполненной работе и предоставьте его преподавателю.

### **Задача 3.**

Скопировать со съемного носителя на жесткий диск компьютера файлы, которые можно будет удалять и восстанавливать с помощью программы Rescuva. Запишите месторасположение скопированных файлов на диске компьютера. Удалите скопированные файлы. Запустите процесс сканирования удаленных файлов. Восстановите файлы, которые необходимо восстановить. Восстановите выбранные файлы. Удалите с помощью программы Rescuva без возможности восстановления. Проверьте отсутствие возможности восстановления файлов с помощью программы Rescuva.

Оформите отчет о выполненной работе и предоставьте его преподавателю.

#### **Творческие задания по дисциплине «Информационная безопасность»**

1. Информатизация общества и проблемы защиты информации.
2. Информационная безопасность и средства массовой информации.
3. Уголовный кодекс и законодательство Российской Федерации в области компьютерных преступлений.
4. Информационная безопасность и права человека.
5. Законодательство Российской Федерации в области защиты информации.
6. Законодательство зарубежных стран в области защиты информации.
7. Система нормативно-правовых актов по обеспечению информационной безопасности Российской Федерации и механизмы ее реализации.
8. Закон Российской Федерации от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации".
9. Система нормативно-правовых актов по обеспечению информационной безопасности США.
10. Закон Российской Федерации «О государственной тайне» и механизм его обеспечения.
11. Указ Президента РФ от 5 декабря 2016 г. № 646 “Об утверждении Доктрины информационной безопасности Российской Федерации”.
12. Законодательство Российской Федерации в области коммерческой тайны.
13. Законодательство зарубежных стран в области коммерческой тайны.
14. Защита информации в работе финансовых организаций и банковских учреждений.
15. Информационная безопасность предприятия (организации).
16. Назначение и структура органов конфиденциального делопроизводства на предприятии.
17. Порядок документирования конфиденциальной информации на различных носителях.
18. Соотношение «секретного» и «несекретного» в условиях демократического государства.

#### **Темы эссе по дисциплине «Информационная безопасность»**

1. Угрозы информации в персональных ЭВМ.
2. Угрозы персональным ЭВМ от компьютерных вирусов.
3. Общие принципы защиты программных продуктов от вирусов.
4. Способы защиты информации в персональных ЭВМ от компьютерных вирусов.
5. Защита компьютерной информации от несанкционированного доступа.
6. Защита компьютерной информации от несанкционированного копирования.
7. Защита информации в сети Интернет.
8. Общие принципы защиты информации в локальных вычислительных сетях.
9. Защита информации в базах данных.
10. Защита информации в операционных системах.
11. Аппаратные средства защиты информации в персональных ЭВМ.
12. Программные средства защиты информации в персональных ЭВМ.
13. Криптографические способы закрытия информации.
14. Защита информации в электронных платежных системах.
15. Государственная система защиты информации, обрабатываемой техническими средствами.

#### **Контрольная работа (аудиторная) – тестирование**

1 Что такое "компьютерный вирус"?



- 1) самостоятельная компьютерная программа или компонент программного комплекса, предназначенная для создания и изменения текстовых файлов.
- 2) это совокупность программ, находящиеся на устройствах долговременной памяти;
- 3) это программы, которые могут "размножаться" и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы;
- 4) это сведения об объектах и явлениях окружающей среды, их параметрах, свойствах и состоянии.

2 Назовите основные типы компьютерных вирусов:

- 1) почтовые, файловые, программные
- 2) аппаратные, программные, загрузочные
- 3) программные, макровирусы, загрузочные.

3 Свойство вируса, позволяющее называться ему загрузочным – способность ...

- 1) заражать загрузочные сектора жестких дисков
- 2) заражать загрузочные дискеты и компакт-диски
- 3) вызывать перезагрузку компьютера-жертвы
- 4) подсвечивать кнопку Пуск на системном блоке.

4 Программа, осуществляющая несанкционированные действия по сбору, и передаче информации злоумышленнику, а также ее разрушение или злонамеренную модификацию это:

- 1) Макровирус
- 2) Сетевой червь
- 3) Троян
- 4) Загрузочный вирус

5 Заражение компьютерными вирусами может произойти в процессе ...

- 1) работы с файлами
- 2) форматирования дискеты
- 3) выключения компьютера
- 4) печати на принтере

6 Какие файлы заражают макро-вирусы?

- 1) исполнительные;
- 2) файлы документов Word и элект. таблиц Excel;
- 3) графические и звуковые;
- 4) html документы.

7 К каким вирусам относится "троянский конь"?

- 1) макро-вирусы
- 2) скрипт-вирусы
- 3) интернет-черви
- 4) загрузочные вирусы.

8 Неопасные компьютерные вирусы могут привести

- 1) к сбоям и зависаниям при работе компьютера;
- 2) к потере программ и данных;
- 3) к форматированию винчестера;
- 4) к уменьшению свободной памяти компьютера.

9 Опасные компьютерные вирусы могут привести...

- 1) к сбоям и зависаниям при работе компьютера;
- 2) к потере программ и данных;
- 3) к форматированию винчестера;
- 4) к уменьшению свободной памяти компьютера.

10 Какой вид компьютерных вирусов внедряются и поражают исполнительный файлы с расширением \*.exe, \*.com и активируются при их запуске?

- 1) файловые вирусы;
- 2) загрузочные вирусы;
- 3) макро-вирусы;
- 4) сетевые вирусы.

11 Какой вид компьютерных вирусов внедряются и поражают файлы с расширением \*.txt, \*.doc?

- 1) файловые вирусы;
- 2) загрузочные вирусы;
- 3) макро-вирусы;
- 4) сетевые вирусы.

12 Как происходит заражение почтовыми вирусами?

- 1) При подключении к web-серверу, зараженному "почтовым" вирусом;
- 2) При открытии зараженного файла, присланного с письмом по e-mail;
- 3) При подключении к почтовому серверу;
- 4) При получении с письма, присланном по e-mail, зараженного файла.

13 Сетевые черви это:

- 1) Вирусы, которые внедряются в документ под видом макросов
- 2) Вирусы, которые проникли на компьютер, блокируют работу сети
- 3) Вредоносные программы, которые проникают на компьютер, используя сервисы компьютерных сетей
- 4) Вредоносные программы, устанавливающие скрытно от пользователя другие программы.

14 Руткит – это:

- 1) Программа для скрытого взятия под контроль взломанной системы
- 2) Вредоносная программа, маскирующаяся под макрокоманду
- 3) Разновидность межсетевого экрана
- 4) Программа, выполняющая несанкционированные действия по передаче управления компьютером удаленному пользователю.

15 Укажите способ заражения компьютерным вирусом при котором осуществляется дописывание тела вируса к концу исполняемого файла.

- 1) заражения файлов исполняемых программ;
- 2) заражения загрузочным вирусом;
- 3) заражения файлов драйверов.
- 4) заражение вирусом из компьютерной сети.

16. Какие программы не относятся к антивирусным?

1. программы-фаги
2. программы-детекторы
3. программы сканирования
4. программы-ревизоры

17. Какая программа не является антивирусной?

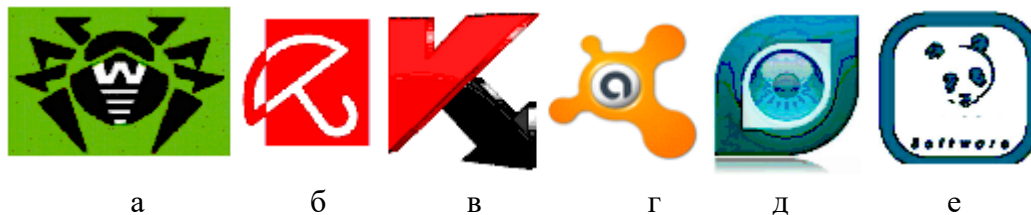
1. Norton Antivirus
2. Dr Web
3. Defrag
4. AVP

18. Отметьте составные части современного антивируса (выберите несколько вариантов правильного ответа)

1. Межсетевой экран
2. Сканер

3. Монитор
4. Модем
5. Принтер

19. Сопоставьте названия программ и изображений



1. Antivir
  2. DrWeb
  3. Nod 32
  4. Antivirus Kaspersky
  5. Avast
  6. Antivirus Panda
20. Выберите правильные утверждения (выберите несколько вариантов правильного ответа)
1. На Web-страницах могут находиться сетевые черви.
  2. Чтобы защитить компьютер недостаточно только установить антивирусную программу.
  3. Если компьютер не подключен к сети Интернет, в него не проникнут вирусы.
  4. Файловые вирусы заражают файлы с расширениями \*.doc, \*.ppt, \*.xls.
  5. Почтовый червь активируется в тот момент, когда к вам поступает электронная почта.
21. Что понимается под сканированием цифровой сигнатуры в антивирусной программе?
1. Локализация и предотвращение вирусных атак, использующих вызовы прерываний.
  2. Распознавание местоположения известных вирусов и их кодов, когда они находятся в памяти.
  3. Сканирование по заданным правилам.
  4. Идентификации уникального цифрового кода вируса.
  5. Вычисление контрольных сумм.
22. Что понимается под мониторингом прерываний в антивирусной программе?
1. Локализация и предотвращение вирусных атак, использующих вызовы прерываний.
  2. Распознавание местоположения известных вирусов и их кодов, когда они находятся в памяти.
  3. Сканирование по заданным правилам.
  4. Идентификации уникального цифрового кода вируса.
  5. Вычисление контрольных сумм.
23. Что понимается под исследованием памяти в антивирусной программе?
1. Локализация и предотвращение вирусных атак, использующих вызовы прерываний.
  2. Распознавание местоположения известных вирусов и их кодов, когда они находятся в памяти.
  3. Сканирование по заданным правилам.
  4. Идентификации уникального цифрового кода вируса.
  5. Вычисление контрольных сумм.
24. Что понимается под эвристическим анализом в антивирусной программе?
1. Локализация и предотвращение вирусных атак, использующих вызовы прерываний.
  2. Распознавание местоположения известных вирусов и их кодов, когда они находятся в памяти.
  3. Сканирование по заданным правилам.
  4. Идентификации уникального цифрового кода вируса.

5. Вычисление контрольных сумм.

25. Что понимается под контролем целостности в антивирусной программе?

1. Локализация и предотвращение вирусных атак, использующих вызовы прерываний.
2. Распознавание местоположения известных вирусов и их кодов, когда они находятся в памяти.
3. Вычисление контрольных сумм.
4. Идентификации уникального цифрового кода вируса.
5. Сканирование по заданным правилам.

26. Какие антивирусные программы осуществляют поиск характерной для конкретного вируса сигнатуры в оперативной памяти и в файлах и при обнаружении выдают соответствующее сообщение?

1. Программы-сканеры.
2. Программы-доктора или фаги.
3. Программы-ревизоры (инспектора).
4. Программы-фильтры (мониторы).
5. Программы-вакцины или иммунизаторы.
6. Программы-детекторы.

27. Какие антивирусные программы проверяют данные на диске на предмет вирусов-невидимок?

1. Программы-детекторы.
2. Программы-доктора или фаги.
3. Программы-ревизоры (инспектора).
4. Программы-фильтры (мониторы).
5. Программы-вакцины или иммунизаторы.
6. Программы-сканеры.

28. Какие антивирусные программы осуществляют резидентные программы, предотвращающие заражение файлов?

1. Программы-детекторы.
2. Программы-доктора или фаги.
3. Программы-ревизоры (инспектора).
4. Программы-фильтры (мониторы).
5. Программы-вакцины или иммунизаторы.
6. Программы-сканеры.

29. Какие антивирусные программы не только находят зараженные вирусами файлы, но и «лечат» их?

1. Программы-детекторы.
2. Программы-доктора или фаги.
3. Программы-ревизоры (инспектора).
4. Программы-фильтры (мониторы).
5. Программы-вакцины или иммунизаторы.
6. Программы-сканеры.

30. Какие антивирусные программы представляют собой небольшие резидентные программы, предназначенные для обнаружения подозрительных действий при работе компьютера, характерных для вирусов?

1. Программы-детекторы.
2. Программы-доктора или фаги.
3. Программы-ревизоры (инспектора).
4. Программы-фильтры (мониторы).
5. Программы-вакцины или иммунизаторы.
6. Программы-сканеры.

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

а) Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

### **основная**

1. Баранова, Е. К. Информационная безопасность и защита информации : Учебное пособие; ВО - Бакалавриат/Национальный исследовательский университет "Высшая школа экономики". - Москва: Издательский Центр РИОР, 2022. - 336 с. - URL: <http://znanium.com/catalog/document?id=393765>.

2. Гришина, Н. В. Информационная безопасность предприятия : Учебное пособие; ВО - Бакалавриат/Российский государственный гуманитарный университет. - Москва: Издательство "ФОРУМ", 2017. - 239 с. - URL: <http://new.znanium.com/go.php?id=612572>.

3. Жук, А. П. Защита информации : учеб. пособие ; ВО - Бакалавриат, Магистратура/Северо-Кавказский федеральный университет; Российский государственный гидрометеорологический университет. - Москва: Издательский Центр РИОР, 2021. - 400 с. - URL: <http://znanium.com/catalog/document?id=367588>.

4. Тумбинская, М. В. Защита информации на предприятии : учебное пособие; ВО - Бакалавриат, Специалитет/Тумбинская М. В., Петровский М. В. - Санкт-Петербург: Лань, 2020. - 184 с. - URL: <https://e.lanbook.com/book/130184>. - Издательство Лань.

### **дополнительная**

5. Нестеров, С. А. Основы информационной безопасности : учебное пособие; ВО - Аспирантура, Бакалавриат, Магистратура, Специалитет/Нестеров С. А. - Санкт-Петербург: Лань, 2022. - 324 с. - URL: <https://e.lanbook.com/book/206279>. - Издательство Лань.

б) Методические материалы, разработанные преподавателями кафедры по дисциплине, в соответствии с профилем ОП.

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

1. Университетская информационная система Россия [Электронный ресурс]. - Режим доступа: <http://uisrussia.msu.ru/>. – Загл. с экрана.

2. Открытое образование [Электронный ресурс]. - Режим доступа: <https://openedu.ru/>. - Загл с экрана.

3. Электронно-библиотечная система Лань [Электронный ресурс]. - Режим доступа: <https://e.lanbook.com/>. – Загл. с экрана.

4. Электронно-библиотечная система Znanium.com [Электронный ресурс]. - Режим доступа: <http://znanium.com/>. – Загл. с экрана.

## 10. Методические указания для обучающихся по освоению дисциплины

Для обеспечения систематической и регулярной работы по изучению дисциплины и успешного прохождения промежуточных и итоговых контрольных испытаний обучающемуся рекомендуется придерживаться следующего порядка обучения:

1. Самостоятельно определить объем времени, необходимого для проработки каждой темы.
2. Регулярно изучать каждую тему дисциплины, используя различные формы индивидуальной работы.
3. Согласовывать с преподавателем виды работы по изучению дисциплины.
4. По завершении отдельных тем передавать выполненные работы (доклады, рефераты, эссе) преподавателю.

Учитывая особенности распределения материала дисциплины, рекомендуется следующая методическая последовательность освоения материала:

1. Сначала обучающийся осваивает основные понятия цифровых технологий и знакомится с особенностями их применения в экономике.

2. После усвоения основных понятий финансов обучающийся знакомится с материалом по темам дисциплины «Информационная безопасность», отраженным в учебно-тематическом плане.

Обучение по дисциплине «Информационная безопасность» предполагает изучение курса на аудиторных занятиях (лекции и практические занятия) и самостоятельной работы обучающихся. Практические занятия дисциплины «Информационная безопасность» предполагают их проведение в различных формах с целью выявления полученных знаний, умений, навыков и компетенций.

Сценарий изучения дисциплины «Информационная безопасность» строится на основе учета нескольких важных моментов:

- очень большой объем дополнительных источников информации;
- широкий спектр информационных технологий, используемых для выполнения практических заданий и приобретения умений и навыков;
- огромный объем справочного материала, подлежащий рассмотрению;
- ограниченное количество учебных часов, отведенное на изучение дисциплины.

В связи с названными проблемами обучение строится следующим образом. На лекциях преподаватель дает общую характеристику рассматриваемого вопроса, различные научные концепции или позиции, которые есть по данной теме. Во время лекции рекомендуется составлять конспект, фиксирующий основные положения лекции и ключевые определения по пройденной теме. Во время лекционного занятия необходимо фиксировать все спорные моменты и проблемы, на которых останавливается преподаватель. Потом именно эти аспекты станут предметом самого пристального внимания и изучения на практических занятиях.

С целью обеспечения успешного обучения обучающийся должен готовиться к лекции, поскольку она является важнейшей формой организации учебного процесса, поскольку:

- знакомит с новым учебным материалом;
- разъясняет учебные элементы, трудные для понимания;
- систематизирует учебный материал;
- ориентирует в учебном процессе.

*Подготовка к лекции* заключается в следующем:

- внимательно прочитайте материал предыдущей лекции;
- узнайте тему предстоящей лекции (по тематическому плану, по информации лектора);
- ознакомьтесь с учебным материалом по рекомендованным источникам;
- постарайтесь уяснить место изучаемой темы в своей профессиональной подготовке;
- запишите возможные вопросы, которые вы зададите лектору на лекции.

*Подготовка к практическим занятиям* заключается в следующем:

- внимательно прочитайте материал лекций, относящихся к данному практическому занятию, ознакомьтесь с учебным материалом по рекомендованным источникам и рабочей тетради;
- выпишите основные термины;
- ответьте на контрольные вопросы по практическим занятиям, готовьтесь дать развернутый ответ на каждый из вопросов;
- проведение расчетов, решение задач, упражнений в рабочей тетради.

*Самостоятельная работа* по дисциплине «Информационная безопасность» включает:

- работу с первоисточниками;
- подготовку устного выступления на практическом занятии;
- подготовку к занятию в интерактивной форме;
- подготовку эссе;
- подготовку презентаций к выступлениям;
- заполнение рабочей тетради;
- работу с тестовыми заданиями;
- подготовку выступлений на студенческих конференциях, для конкурсов студенческих работ;
- подготовку к текущему, рубежному контролю и промежуточной аттестации по дисциплине.

*Написание доклада, эссе.*

*Доклад* - публичное сообщение, представляющее собой развернутое изложение определенной темы.

Доклад должен включать введение, главную часть и заключение. Во введении кратко излагается значение рассматриваемого вопроса в научном и учебном плане, применительно к теме занятия. Затем излагаются основные положения проблемы и делаются заключение и выводы. В конце работы дается подробный перечень литературных источников, которыми пользовался обучающийся при написании реферата или доклада.

В рамках самостоятельной работы предусмотрено выполнение студентом доклада оформленного в виде презентации. По объему доклад должен составлять 5-7 слайдов. Доклад по объему должен составлять 3-5 страниц машинописного текста, кегль 14, межстрочный интервал 1,5 строки.

Превышение указанного объема (как правило) рассматривается, как неумение автора систематизировать материал.

*Эссе* - прозаическое сочинение свободной композиции, носящее исследовательский характер и выражающее:

- индивидуальные впечатления по конкретному вопросу,
- соображения по конкретному вопросу,
- выявление и видение проблем и противоречий. Здесь важно показать наличие противоречий или проблемы (увиденных автором эссе или выявленных другими авторами) и возможные пути их разрешения.

В эссе обязателен список использованной литературы и ссылка на используемые источники информации по общепринятым правилам. Примерная структура эссе:

- начало эссе - краткое изложение сути вопроса, проблемы;
- основная часть эссе - видение путей решения проблемы;
- конец эссе - резюме автора эссе по конкретному вопросу, проблеме.

В соотношении реферативной и исследовательской частей первая не должна превышать 50%. В случае простого реферирования «Эссе» либо не оценивается, либо оценивается минимальным количеством баллов.

Содержание эссе, предполагающие расчёты должны опираться на конкретные примеры из специализированных периодических изданий или других источников.

По объему эссе должно составлять 5-7 страниц машинописного текста, кегль 14, межстрочный интервал 1,5 строки. Превышение указанного объема (как правило) рассматривается как неумение автора систематизировать материал.

По дисциплине «Информационная безопасность» предусмотрен *зачет*. К зачету допускаются студенты, выполнившие и сдавшие практические работы по дисциплине, имеющие ежемесячную аттестацию и наличие по текущей успеваемости более 45 баллов. Студентам, набравшим более 55 баллов, зачет выставляется по результатам текущей успеваемости, студенты, набравшие от 45 до 54 баллов, сдают зачет по вопросам, предусмотренным РПД.

При проведении итоговой аттестации «зачет» преподавателю с согласия студента разрешается выставлять оценку «зачет» по результатам набранных баллов в ходе текущего контроля успеваемости в семестре по выше приведенной шкале.

В случае отказа – студент сдает зачет по приведенным выше вопросам и заданиям. Итоговая успеваемость *зачет* не может оцениваться ниже суммы баллов, которую студент набрал по итогам текущей и промежуточной успеваемости.

При сдаче *зачета* к заработанным в течение семестра студентом баллам прибавляются баллы, полученные на *зачете* и сумма баллов переводится в оценку.

**11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства и информационных справочных систем (при необходимости).**

**11.1 Перечень лицензионного программного обеспечения**

№ п/п	Наименование	Условия доступа
1	Microsoft Windows	из внутренней сети университета (лицензионный договор)
2	Microsoft Office	из внутренней сети университета (лицензионный договор)
3	Антивирус Касперского	из внутренней сети университета (лицензионный договор)
4	Консультант Плюс	из внутренней сети университета (лицензионный договор)
5	Гарант	из внутренней сети университета (лицензионный договор)
6	СДО MOODLE	из любой точки, в которой имеется доступ к сети Интернет (лицензионный договор)

**11.2 Перечень свободно распространяемого программного обеспечения**

№ п/п	Наименование	Условия доступа
1	Zoom Video Communications, Inc. (Zoom) <a href="https://explore.zoom.us/ru/products/meetings/">https://explore.zoom.us/ru/products/meetings/</a>	из внутренней сети университета (свободный доступ)

**11.3 Перечень программного обеспечения отечественного производства**

При осуществлении образовательного процесса студентами и преподавателем используются следующие информационно справочные системы: СПС «Консультант плюс», СПС «Гарант».

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

№ п/п	Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы
1	<b>Учебная аудитория для проведения лекционных занятий</b> (ауд. № 160, площадь – 202,7 м <sup>2</sup> ).	Специализированная мебель на 180 посадочных мест, персональный компьютер – 1 шт., проектор Panasonic EX620 X6A – 1 шт., интерактивная доска SMART Board 690 – 1 шт., трибуна для лектора – 1 шт., микрофон – 1 шт., мониторы - 3 шт., плазменная панель - 1 шт., учебно-наглядные пособия в виде презентаций, информационные плакаты, подключение к сети «Интернет», выход в корпоративную сеть университета.
2	<b>Учебная аудитория для проведения занятий семинарского типа</b> (ауд. № 165, площадь – 66,6 м <sup>2</sup> ).	Специализированная мебель на 30 посадочных мест, персональные компьютеры – 13 шт., мультимедийный проектор – 1 шт., телевизор SAMSUNG UHD TV 7 series - 1 шт., учебно-наглядные пособия в виде презентаций, информационные плакаты, подключение к сети «Интернет», доступ в электронную информационно-образовательную среду университета, выход в корпоративную сеть университета.
3	<b>Учебные аудитории для самостоятельной работы студентов:</b>	
	<i>1. Читальный зал научной библиотеки (площадь 177 м<sup>2</sup>)</i>	Оснащение: специализированная мебель на 100 посадочных мест, персональные компьютеры – 56 шт., телевизор – 1шт., принтер – 1шт., цветной принтер – 1шт., копировальный аппарат – 1шт., сканер – 1шт., Wi-Fi оборудование, подключение к сети «Интернет», доступ в электронную



		информационно-образовательную среду университета, выход в корпоративную сеть университета.
	2. Учебная аудитория № 165 (площадь – 66,6 м <sup>2</sup> )	Специализированная мебель на 30 посадочных мест, персональные компьютеры – 13 шт., мультимедийный проектор – 1 шт., телевизор SAMSUNG UHD TV 7 series - 1 шт., учебно-наглядные пособия в виде презентаций, информационные плакаты, подключение к сети «Интернет», доступ в электронную информационно-образовательную среду университета, выход в корпоративную сеть университета.
4	<b>Учебная аудитория для групповых и индивидуальных консультаций</b> (ауд. № 165, площадь – 66,6 м <sup>2</sup> ).	Специализированная мебель на 30 посадочных мест, персональные компьютеры – 13 шт., мультимедийный проектор – 1 шт., телевизор SAMSUNG UHD TV 7 series - 1 шт., учебно-наглядные пособия в виде презентаций, информационные плакаты, подключение к сети «Интернет», доступ в электронную информационно-образовательную среду университета, выход в корпоративную сеть университета.
5	<b>Учебная аудитория для текущего контроля и промежуточной аттестации</b> (ауд. № 165, площадь – 66,6 м <sup>2</sup> ).	Специализированная мебель на 30 посадочных мест, персональные компьютеры – 13 шт., мультимедийный проектор – 1 шт., телевизор SAMSUNG UHD TV 7 series - 1 шт., учебно-наглядные пособия в виде презентаций, информационные плакаты, подключение к сети «Интернет», доступ в электронную информационно-образовательную среду университета, выход в корпоративную сеть университета.

### 13. Особенности реализации дисциплины лиц с ограниченными возможностями здоровья

Обучающимся с ограниченными возможностями здоровья предоставляются специальные учебники и учебные пособия, иная учебная литература, специальные технические средства обучения коллективного и индивидуального пользования, предоставление услуг ассистента (помощника), оказывающего обучающимся необходимую техническую помощь, а также услуги сурдопереводчиков и тифлосурдопереводчиков.

#### а) для слабовидящих:

- на промежуточной аттестации присутствует ассистент, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (он помогает занять рабочее место, передвигаться, прочитать и оформить задание, в том числе записывая под диктовку);

- задания для выполнения, а также инструкция о порядке проведения промежуточной аттестации оформляются увеличенным шрифтом;

- задания для выполнения на промежуточной аттестации зачитываются ассистентом;

- письменные задания выполняются на бумаге, надиктовываются ассистенту;

- обеспечивается индивидуальное равномерное освещение не менее 300 люкс;

- студенту для выполнения задания при необходимости предоставляется увеличивающее устройство;

#### в) для глухих и слабослышащих:

- на промежуточной аттестации присутствует ассистент, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (он помогает занять рабочее место, передвигаться, прочитать и оформить задание, в том числе записывая под диктовку);

- промежуточная аттестация проводится в письменной форме;

- обеспечивается наличие звукоусиливающей аппаратуры коллективного пользования, при необходимости поступающим предоставляется звукоусиливающая аппаратура индивидуального пользования;

- по желанию студента промежуточная аттестация может проводиться в письменной форме;

**д) для лиц с нарушениями опорно-двигательного аппарата (тяжелыми нарушениями двигательных функций верхних конечностей или отсутствием верхних конечностей):**

- письменные задания выполняются на компьютере со специализированным программным обеспечением или надиктовываются ассистенту;

- по желанию студента промежуточная аттестация проводится в устной форме.

Рабочая программа дисциплины «Информационная безопасность» составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки 38.03.01 «Экономика» и учебного плана по направлению 38.03.01 «Экономика» профилю «Экономика предприятий и организаций».

Автор к.т.н., профессор Жук А.П.

Рецензенты к.т.н., доцент Трошков А.М.

к.т.н., доцент Рачков В.Е.

Рабочая программа дисциплины «Информационная безопасность» рассмотрена на заседании кафедры информационных систем протокол №11 от 12 мая 2022 г. и признана соответствующей требованиям ФГОС ВО по направлению подготовки 38.03.01 «Экономика» и учебного плана по направлению 38.03.01 «Экономика» профилю «Экономика предприятий и организаций».

Зав. кафедрой информационных систем,  
канд. техн. наук, доцент

Хабаров А.Н.

Рабочая программа дисциплины «Информационная безопасность» рассмотрена на заседании учебно-методической комиссии экономического факультета протокол № 9 от 19 мая 2022 г. и признана соответствующей требованиям ФГОС ВО по направлению подготовки 38.03.01 «Экономика» и учебного плана по направлению 38.03.01 «Экономика» профилю «Экономика предприятий и организаций».

Руководитель ОП, к.э.н.,  
доцент

Токарева Г.В.

**Аннотация рабочей программы дисциплины**  
**«Информационная безопасность»**  
 по подготовке обучающегося по программе бакалавриата  
 по направлению подготовки

<b>38.04.01</b>	<b>Экономика</b>
код	Наименование направления подготовки
	<b>Экономика предприятий и организаций</b>
	профиль
Форма обучения – <b>очная, очно-заочная.</b> Общая трудоемкость изучения дисциплины составляет – 2 з.е., 72 час.	
<b>Программой дисциплины предусмотрены следующие виды занятий</b>	<b>Очная форма обучения:</b> лекции – 18 ч., в том числе практическая подготовка - 18 ч., практические (лабораторные) занятия – 18 ч., в том числе практическая подготовка - 18 ч., самостоятельная работа – 36 ч., в том числе практическая подготовка - 36 ч. <b>Очно-заочная форма обучения:</b> лекции – 14 ч., в том числе практическая подготовка - 14 ч., практические (лабораторные) занятия – 14 ч., в том числе практическая подготовка - 14 ч., самостоятельная работа – 44 ч., в том числе практическая подготовка - 44 ч.
<b>Цель изучения дисциплины</b>	Формирование у студентов бакалавриата теоретических знаний и практических навыков по защищённому сбору, обработке и мониторингу исходных данных, необходимых для проведения анализа и планирования показателей производственной, коммерческой и финансово-экономической деятельности организации. Студенты знакомятся с понятием информационная безопасность и защита информации, методами и средствами обеспечения информационной безопасности производственной, коммерческой и финансово-экономической информации организации, порядком их применения в предстоящей профессиональной деятельности.
<b>Место дисциплины в структуре ОП ВО</b>	Учебная дисциплина Б1.В.ДВ.03.02 «Информационная безопасность» является дисциплиной по выбору части, формируемой участниками образовательных отношений программы бакалавриата.
<b>Компетенции и индикатор (ы) достижения компетенций, формируемые в результате освоения дисциплины</b>	<b>Профессиональные (ПК):</b> <b>ПК-1. Сбор, мониторинг и обработка данных для проведения расчетов экономических показателей организации</b> <i>ПК-1.1</i> Способен выполнять работы по сбору, обработке и мониторингу исходных данных, необходимых для проведения анализа и планирования показателей производственной, коммерческой и финансово-экономической деятельности организации. <i>ПК-2.1</i> Обосновывает и применяет статистические, экономико-математические, маркетинговые методы исследования внешней среды и деятельности организации, проводит расчеты финансово-экономических показателей, в т.ч. с использованием типовых методик и нормативно-правовых актов.
<b>Знания, умения и навыки, получаемые в процессе изучения дисциплины</b>	<b>Знания:</b> - методов и приемов сбора, обработки и мониторинга исходных данных, необходимых для проведения анализа и планирования показателей производственной, коммерческой и финансово-экономической деятельности организации с учетом требований информационной безопасности (ПК-1.1). - методов проведения статистических, экономико-математических, маркетинговых исследований внешней среды и деятельности организации с учетом требований информационной безопасности (ПК-2.1). <b>Умения:</b>

	<p>- осуществлять работы по сбору, обработке и мониторингу исходных данных, необходимых для проведения анализа и планирования показателей производственной, коммерческой и финансово-экономической деятельности организации с учетом требований информационной безопасности (ПК-1.1).</p> <p>- проводить статистические, экономико-математические, маркетинговые методы исследования внешней среды и деятельности организации с учетом требований информационной безопасности (ПК-2.1).</p> <p><b>Навыки или трудовые действия:</b></p> <p>- сбора, обработки и мониторинга показателей производственной, коммерческой и финансово-экономической деятельности организации с учетом требований информационной безопасности (ПК-1.1)</p> <p>- решения типовых задач проведения расчетов финансово-экономических показателей организации, в т.ч. с использованием типовых методик и нормативно-правовых актов (ПК-1.2).</p>
<b>Краткая характеристика учебной дисциплины (основные разделы и темы)</b>	<p>Тема № 1 Введение в дисциплину.</p> <p>Тема №2 Уязвимости и угрозы информационной безопасности.</p> <p>Тема №3 Каналы утечки конфиденциальной информации.</p> <p>Тема № 4 Способы несанкционированного доступа к конфиденциальной информации.</p> <p>Тема № 5 Аутентификация и методы защиты информации.</p> <p>Тема № 6 Удаленные атаки в компьютерных сетях.</p> <p>Тема № 7 Компьютерные вирусы и способы борьбы с ними.</p> <p>Тема № 8 Персонал как основная опасность утраты конфиденциальной информации.</p> <p>Тема № 9 Политика информационной безопасности организации.</p>
<b>Форма контроля</b>	<p><u>Очная форма обучения:</u> семестр 7 – зачет</p> <p><u>Очно-заочная форма обучения:</u> семестр 8 – зачет</p>
<b>Автор:</b>	<p>профессор кафедры информационных систем, к.т.н., профессор А.П. Жук</p>