Министерство сельского хозяйства Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ЛУГАНСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ ИМЕНИ К.Е. ВОРОШИЛОВА»

«Утверждаю»
Декан факультета экономики и управления АПК

Шевченко М.Н. _____
«25» апреля 2025 г.

РАБОЧАЯ ПРОГРАММА

учебной дисциплины «Информационная безопасность»

для направления подготовки 38.03.05 Бизнес-информатика

направленность (профиль) Бизнес-информатика

Год начала подготовки – 2025

Квалификация выпускника – бакалавр

Луганск, 2025

Рабочая программа составлена с учетом требований:

- порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 06.04.2021 № 245 (с изменениями и дополнениями);
- федерального государственного образовательного стандарта высшего образования – бакалавриат по направлению подготовки 38.03.05 Бизнес- информатика, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 29.07.2020г. № 838 (с изменениями и дополнениями).

Преподаватели, подготовившие рабочую программу:

старший преподаватель _____ **Ю.А. Горячкова**
кафедры информационных технологий,
математики и физики

Рабочая программа рассмотрена на заседании кафедры информационных технологий, математики и физики (протокол № 8 от «07» апреля 2025 г.).

Заведующий кафедрой _____ **В.Ю. Ильин**

Рабочая программа рекомендована к использованию в учебном процессе методической комиссией факультета экономики и управления АПК (протокол № 8 от «24» апреля 2025 г.).

Председатель методической комиссии _____ **А.В. Худолей**

Руководитель основной профессиональной образовательной программы _____ **В.Ю. Ильин**

1. Предмет. Цели и задачи дисциплины, её место в структуре образовательной программы

Предмет дисциплины включает:

– основы правового регулирования отношений в информационной сфере;

– конституционные гарантии прав граждан на получение информации и механизм их реализации;

– понятия и виды защищаемой информации по законодательству РФ;

систему защиты государственной тайны;

– основы правового регулирования отношений в области интеллектуальной собственности и способы защиты этой собственности;

– понятие и виды компьютерных преступлений.

Цель изучения дисциплины: формирование у студентов навыков, связанных с обеспечением защиты информации; творческих подходов при решении сложных научно-технических задач, связанных с обеспечением информационной безопасности объектов информатизации; создание представления об основах информационной безопасности, принципах и методах противодействия несанкционированному информационному воздействию; развитие способностей к логическому и алгоритмическому мышлению.

Задачи изучения дисциплины:

– изучить место и роль информационной безопасности в системе национальной безопасности;

– изучить основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы в данной области; технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации;

– освоить принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации;

– сформировать умения и навыки проведения анализа и оценки угроз информационной безопасности объекта;

– получить навыки работы с современными технологиями обеспечения информационной безопасности.

Место дисциплины в структуре образовательной программы.

Дисциплина «Информационная безопасность» относится к части, формируемой участниками образовательных отношений (Б1.В.06) блока дисциплин подготовки студентов по направлению подготовки 38.03.05 Бизнес-информатика, направление подготовки Бизнес-информатика основой профессиональной образовательной программы высшего образования (далее – ОПОП ВО).

Дисциплина реализуется кафедрой информационных технологий, математики и физики в 6 и 7 семестрах. Основывается на базе дисциплин: «Современные информационные технологии и системы искусственного интеллекта», «Базы данных».

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

Коды компетенций	Формулировка компетенции	Индикаторы достижения компетенции	Планируемые результаты обучения
ПК-1	Способен формировать возможные решения на основе разработанных для них целевых показателей с учетом имеющихся факторов, условий и рисков и анализа требований заинтересованных сторон с точки зрения выбранных критериев	**ПК–1.1.** Осуществляет выявление, сбор, систематизацию, хранение, поддержание в актуальном состоянии, анализ, определение зависимости между элементами информации бизнес-анализа для формирования возможных решений используя современные методы исследования и применяя информационные технологии	**Знать:** назначение и функции информационных технологий и современных программных продуктов для решения профессиональных задач **иметь:** определять назначение и функции информационных систем и технологий для решения профессиональных задач **иметь навыки:** работы с информационными системами и технологиями для решения профессиональных задач
		ПК-1.4. Составляет описание возможных решений в соответствии с выбранными подходами с учетом имеющихся факторов, условий и рисков	**Знать:** информационные технологии и программные средства для решения профессиональных задач **уметь:** применять информационные технологии и программные средства для решения профессиональных задач **иметь навыки:** применения информационные технологии и программные средства для решения профессиональных задач
ПК-2	Способен проводить анализ, обоснование и выбор решения с использованием информационных	**ПК-2.1.** Проводит анализ решений и оценку ресурсов, необходимых для реализации решения с точки зрения	**Знать:** методы сбора, анализа, систематизации информации о факторах внешней и внутренней среды предприятия; **уметь:** анализировать

	технологий и современных методов исследования	достижения целевых показателей решений	внутренние (внешние) факторы и условия, влияющие на деятельность организации; **иметь навыки:** разработки этапов принятия управленческих решений рациональным методом; анализ факторов, влияющих на процесс принятия решений
		ПК-2.3. Применяет информационные технологии (программные средства и платформы) инфраструктуры информационных технологий организаций, используя современные подходы и стандарты автоматизации, в объеме, необходимом для целей бизнес анализа и адаптации бизнес- процессов заказчика к возможностям информационной системы	**Знать:** цели и задачи стратегических изменений в организации, основные параметры и ключевые показатели эффективности разрабатываемых стратегических изменений в организации; **уметь:** проводить оценку вариантов разрабатываемых стратегий с точки зрения выбранных критериев; **иметь навыки:** оценки эффективности реализации стратегии по результатам деятельности предприятия с точки зрения реализации выбранных целей

3. Объём дисциплины и виды учебной работы

Виды работ	Очная форма обучения			Заочная форма обучения	Очно-заочная форма обучения	
	всего	в т.ч. по семестрам		всего часов	всего часов	
		6 семестр	7 семестр	–	8 семестр	9 семестр
Общая трудоёмкость дисциплины, зач.ед./часов, в том числе:	7/252	3/108	4/144	–	3/108	4/144
Контактная работа, часов:	84	36	48	–	22	30
- лекции	42	18	24	–	10	14
- практические (семинарские) занятия	42	18	24	–	12	16
- лабораторные работы	–	–	–	–	–	
Самостоятельная работа, часов	168	72	96	–	86	114
Контроль, часов	–	–	–	–	–	
Вид промежуточной аттестации (зачёт, экзамен)	зачет/ экзамен	зачет	экзамен	–	зачет	экзамен

4. Содержание дисциплины

4.1. Разделы дисциплины и виды занятий (тематический план)

Раздел дисциплины (тема)	Л	ПЗ	ЛР	СРС
Очная форма обучения				
Тема 1. Теоретические основы информационной безопасности	2	2	–	14
Тема 2. Государственная система информационной безопасности. Законодательство в области информационной безопасности	4	4	–	14
Тема 3. Риски и угрозы информационной безопасности	4	4	–	14
Тема 4. Организационное обеспечение информационной безопасности	2	2	–	14
Тема 5. Технические средства и методы защиты информации	4	4	–	14
Тема 6. Средства антивирусной защиты информации	4	4	–	14
Тема 7. Средства восстановления данных	4	4	–	14
Тема 8. Политика информационной безопасности организации (предприятия)	2	2	–	14
Тема 9. Электронный документооборот, основные понятия и требования безопасности	4	4	–	14
Тема 10. Теоретические и организационные основы систем электронного документооборота организации	4	4	–	14
Тема 11. Экономические аспекты информационной	4	4	–	14

безопасности				
Тема 12. Информационная безопасность в социально-экономических системах	4	4	–	14
Всего	**42**	**42**	**–**	**168**
Заочная форма обучения				
–	–	–	–	–
Очно-заочная форма обучения				
Тема 1. Теоретические основы информационной безопасности	2	2	–	16
Тема 2. Государственная система информационной безопасности. Законодательство в области информационной безопасности	2	2	–	16
Тема 3. Риски и угрозы информационной безопасности	2	2	–	16
Тема 4. Организационное обеспечение информационной безопасности	2	2	–	16
Тема 5. Технические средства и методы защиты информации	2	2	–	16
Тема 6. Средства антивирусной защиты информации	2	4	–	16
Тема 7. Средства восстановления данных	2	4	–	16
Тема 8. Политика информационной безопасности организации (предприятия)	2	2	–	18
Тема 9. Электронный документооборот, основные понятия и требования безопасности	2	2	–	18
Тема 10. Теоретические и организационные основы систем электронного документооборота организации	2	2	–	18
Тема 11. Экономические аспекты информационной безопасности	2	2	–	18
Тема 12. Информационная безопасность в социально-экономических системах	2	2	–	16
Всего	**24**	**28**	**–**	**200**

4.2. Содержание разделов учебной дисциплины

Тема 1. Теоретические основы информационной безопасности. Составляющие информационной безопасности. Доступность информации. Целостность информации. Конфиденциальность информации.

Тема 2. Государственная система информационной безопасности. Законодательство в области информационной безопасности Правовое обеспечение информационной безопасности. Доктрина информационной безопасности Российской Федерации. Концепция информационной безопасности сетей связи общего пользования Российской Федерации. Вопрос правового обеспечения информационной безопасности в Российской Федерации.

Тема 3. Риски и угрозы информационной безопасности. Информационные угрозы: понятие, виды и причины. Предпосылки появления угроз. Основные направления и методы реализации угроз. Характер происхождения угроз (умышленные и естественные факторы). Методики оценки рисков в сфере информационной безопасности. Технологии (методики) управления информационными рисками. Роль государства в минимизации рисков и угроз информационной безопасности. Программное обеспечение для оценки

рисков информационной безопасности. Аудит безопасности и анализ информационных рисков. Построение систем защиты от угрозы нарушения конфиденциальности. Построение систем защиты от угрозы нарушения целостности информации и отказа доступа.

Тема 4. Организационное обеспечение информационной безопасности. Основные понятия организационного обеспечения информационной безопасности. Административный уровень информационной безопасности. Программа безопасности. Уровни детализации политики информационной безопасности.

Тема 5. Технические средства и методы защиты информации. Оценка безопасности информационных систем. Структура системы информационной безопасности. Программно-аппаратные средства и методы обеспечения информационной безопасности. Аппаратные средства защиты информации. Вспомогательные аппаратные средства защиты информации. Основные и вспомогательные программные средства защиты информации.

Тема 6. Средства антивирусной защиты информации. Средства антивирусной защиты информации. Источники вирусов. Признаки заражения и антивирусные программы. Критерии выбора антивирусного программного обеспечения.

Тема 7. Средства восстановления данных. Способы восстановления данных. Средства резервного копирования, восстановления, защиты данных. Критерии выбора программного обеспечения для восстановления данных.

Тема 8. Политика информационной безопасности организации (предприятия). Анализ структурно-функциональных особенностей предприятия с точки зрения политики безопасности. Теоретические основы построения моделей политики информационной безопасности. Формирование оценки угрозы доступности, целостности, конфиденциальности на предприятии.

Тема 9. Электронный документооборот, основные понятия и требования безопасности. Основные термины и определения. Этапы документооборота. Представление о системе электронного документооборота. Требования к системам электронного документооборота. Отечественные и международные стандарты организации электронного документооборота.

Тема 10. Теоретические и организационные основы систем электронного документооборота организации. Структура, задачи и функции информационной системы электронного документооборота. Юридическая сила электронного документа. Проблема защиты информации и информационной безопасности в системах электронного документооборота. Защита персональных данных в информационных системах. Реализованные проекты внедрения систем электронного документооборота в ведомствах и негосударственных структурах РФ. Общегосударственные информационные системы. Критерии выбора программного обеспечения для системы электронного документооборота.

Тема 11. Экономические аспекты информационной безопасности. Экономические факторы и их роль в обеспечении информационной безопасности. Методики оценки экономической эффективности системы обеспечения информационной безопасности. Элементы управления кибербезопасности автоматизированных систем. Управление рисками информационной безопасности. Экономические последствия нарушений информационной безопасности.

Тема 12. Информационная безопасность в социально-экономических системах. Уровни информационной безопасности. Влияние цифровизации на национальную безопасность. Информационная безопасность в финансовой сфере. Обеспечение информационной безопасности данных и систем электронного документооборота. Влияние цифровизации на информационную безопасность хозяйствующих субъектов. Управление информационной безопасностью в хозяйствующих субъектах: политика, процессы и стандарты.

4.3. Перечень тем лекций

№ п/п	Тема лекции	Объём, ч		
		форма обучения		
		очная	заочная	очно-заочная
1.	Тема лекционного занятия 1. Теоретические основы информационной безопасности	2	–	2
2.	Тема лекционного занятия 2. Государственная система информационной безопасности.	4	–	2
3.	Тема лекционного занятия 3. Риски и угрозы информационной безопасности	4	–	2
4.	Тема лекционного занятия 4. Организационное обеспечение информационной безопасности	2	–	2
5.	Тема лекционного занятия 5. Технические средства и методы защиты информации	4	–	2
6.	Тема лекционного занятия 6. Средства антивирусной защиты информации	4	–	2
7.	Тема лекционного занятия 7. Средства восстановления данных	4	–	2
8.	Тема лекционного занятия 8. Политика информационной безопасности организации	2	–	2
9.	Тема лекционного занятия 9. Электронный документооборот, основные понятия и требования безопасности	4	–	2
10.	Тема лекционного занятия 10. Теоретические и организационные основы систем электронного документооборота организации	4	–	2
11.	Тема лекционного занятия 11. Экономические аспекты информационной безопасности	4	–	2
12.	Тема лекционного занятия 12. Информационная безопасность в социально-экономических системах	4	–	2
Всего		**42**	**–**	**24**

4.4. Перечень тем практических (семинарских) занятий

№ п/п	Тема практического (семинарского) занятия	Объём, ч		
		форма обучения		
		очная	заочная	очно-заочная
1.	Тема практического занятия 1. Правовые основы информационной безопасности и защиты	2	–	2
2.	Тема практического занятия 2. Антивирусная защита данных	4	–	2

3.	Тема практического занятия 3. Восстановление данных	4	–	2
4.	Тема практического занятия 4. Разграничение прав доступа системы	2	–	2
5.	Тема практического занятия 5. Файловые подсистемы	4	–	2
6.	Тема практического занятия 6. Обеспечение целостности и доступности данных	4	–	4
7.	Тема практического занятия 7. Настройки безопасности интернет обозревателей	4	–	4
8.	Тема практического занятия 8. Организация защищенной системы электронной почты	2	–	2
9.	Тема практического занятия 9. Безопасность на уровне операционной системы и приложений	4	–	2
10.	Тема практического занятия 10. Установка и первоначальная настройка VM VirtualBox	4	–	2
11.	Тема практического занятия 11. Практика применения электронного документооборота.	4	–	2
12.	Тема практического занятия 12. Защита информации в системах электронного документооборота	4	–	2
Всего		**42**	**–**	**28**

4.5. Перечень тем лабораторных работ.

Не предусмотрены.

4.6. Виды самостоятельной работы студентов и перечень учебно-методического обеспечения для самостоятельной работы обучающихся

4.6.1. Подготовка к аудиторным занятиям

Материалы лекций являются основой для изучения теоретической части дисциплины и подготовки студента к практическим занятиям.

При подготовке к аудиторным занятиям студент должен:

- изучить рекомендуемую литературу;
- просмотреть самостоятельно дополнительную литературу по изучаемой теме.

Основной целью практических занятий является изучение отдельных наиболее сложных и интересных вопросов в рамках темы, а также контроль за степенью усвоения пройдённого материала и ходом выполнения студентами самостоятельной работы.

4.6.2. Перечень тем курсовых работ (проектов)

Не предусмотрены.

4.6.3. Перечень тем рефератов, расчетно-графических работ и иных видов индивидуальных работ

Не предусмотрены.

4.6.4. Перечень тем и учебно-методического обеспечения для самостоятельной работы обучающихся

№ п/п	Тема самостоятельной работы	Учебно-методическое обеспечение	Объём, ч
			форма обучения

№	Тема самостоятельной	Учебно-методическое обеспечение	Объём, ч		
			очная	заочная	очно-заочная
1.	Теоретические основы информационной безопасности	1. Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс] : учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - Москва : РИОР, 2013. - 222 с. - ISBN 978-5-369-01178-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/405000 (дата обращения: 06.03.2025). – Режим доступа: по подписке. 2. Информационная безопасность и зашита информации : учебное пособие для направления подготовки 40.03.01 - Юриспруденция, специальности 40.05.02 - Правоохранительная деятельность, специальности 37.05.02 - Психология служебной деятельности, очной и заочной форм обучения / О. А. Панфилова, Д. Ю. Крюкова, А. Н. Наимов, В. В. Мухин ; Федер. служба исполн. наказаний, Вологод. ин-т права и экономики. - Вологда : ВИПЭ ФСИН России, 2018. - 59 с. - ISBN 978-5-94991-428-1. - Текст : электронный. - URL: https://znanium.com/catalog/product/1229037 (дата обращения: 06.03.2025). – Режим доступа: по подписке. 3. Попов, И. В. Информационная безопасность : практикум / И. В. Попов, Н. И. Улендеева. - Самара : Самарский юридический институт ФСИН России, 2022. - 90 с. - ISBN 978-5-91612-375-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/2016193 (дата обращения:	14	–	16
2.	Государственная система информационной безопасности. Законодательство в области информационной безопасности		14	–	16
3.	Риски и угрозы информационной безопасности		14	–	16
4.	Организационное обеспечение информационной безопасности		14	–	16
5.	Технические средства и методы защиты информации		14	–	16
6.	Средства антивирусной защиты информации		14	–	16
7.	Средства восстановления данных		14	–	16
8.	Политика информационной безопасности организации (предприятия)		14	–	18

№	Тема самостоятельной	Учебно-методическое обеспечение	Объём, ч		
9.	Электронный документооборот, основные понятия и требования безопасности	06.03.2025). – Режим доступа: по подписке. 4. Рычаго, М. Е. Основы защиты информации : учебное пособие / М. Е. Рычаго, И. В. Ершова, Р. Н. Тихомиров. - Владимир : ВЮИ ФСИН России, 2017. - 68 с. - ISBN 978-5-93035-622-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1864501 (дата обращения: 06.03.2025). – Режим доступа: по подписке. 5. Абрамов, В. Ю. Цифровое право : практика применения электронного документооборота в различных сферах общественных коммуникаций : практическое руководство / В. Ю. Абрамов. - Москва : Статут, 2022. - 168 с. - ISBN 978-5-8354-1791-9. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2193849 (дата обращения: 06.03.2025). – Режим доступа: по подписке.	14	–	18
10.	Теоретические и организационные основы систем электронного документооборота организации		14	–	18
11.	Экономические аспекты информационной безопасности		14	–	18
12.	Информационная безопасность в социально-экономических системах		14	–	16
Всего			**168**	**–**	**200**

4.6.5. Другие виды самостоятельной работы студентов

Не предусмотрены.

4.7. Перечень тем и видов занятий, проводимых в интерактивной форме

№ п/п	Форма занятия	Тема занятия	Интерактивный метод	Объем, ч
1.	Лекция	Теоретические основы информационной безопасности	Интерактивная лекция	2

5. Фонд оценочных средств для проведения промежуточной аттестации

Полное описание фонда оценочных средств текущей и промежуточной аттестации обучающихся с перечнем компетенций, описанием показателей и критериев оценивания компетенций, шкал оценивания, типовые контрольные задания и методические материалы представлены в Приложении 3 к настоящей программе.

6. Учебно-методическое обеспечение дисциплины

6.1. Рекомендуемая литература

6.1.1. Основная литература

№ п/п	Автор, название, место издания, изд-во, год издания	Кол-во экз. в библ.
1.	Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс] : учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - Москва : РИОР, 2013. - 222 с. - ISBN 978-5-369-01178-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/405000 (дата обращения: 06.03.2025). – Режим доступа: по подписке.	Электронный ресурс
2.	Информационная безопасность и зашита информации : учебное пособие для направления подготовки 40.03.01 - Юриспруденция, специальности 40.05.02 - Правоохранительная деятельность, специальности 37.05.02 - Психология служебной деятельности, очной и заочной форм обучения / О. А. Панфилова, Д. Ю. Крюкова, А. Н. Наимов, В. В. Мухин ; Федер. служба исполн. наказаний, Вологод. ин-т права и экономики. - Вологда : ВИПЭ ФСИН России, 2018. - 59 с. - ISBN 978-5-94991-428-1. - Текст : электронный. - URL: https://znanium.com/catalog/product/1229037 (дата обращения: 06.03.2025). – Режим доступа: по подписке.	Электронный ресурс
3.	Попов, И. В. Информационная безопасность : практикум / И. В. Попов, Н. И. Улендеева. - Самара : Самарский юридический институт ФСИН России, 2022. - 90 с. - ISBN 978-5-91612-375-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/2016193 (дата обращения: 06.03.2025). – Режим доступа: по подписке.	Электронный ресурс
4.	Рычаго, М. Е. Основы защиты информации : учебное пособие / М. Е. Рычаго, И. В. Ершова, Р. Н. Тихомиров. - Владимир : ВЮИ ФСИН России, 2017. - 68 с. - ISBN 978-5-93035-622-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1864501 (дата обращения: 06.03.2025). – Режим доступа: по подписке.	Электронный ресурс

6.1.2. Дополнительная литература

№ п/п	Автор, название, место издания, изд-во, год издания, количество страниц
1.	Ерохин, В. В. Безопасность информационных систем : учебное пособие / В. В. Ерохин, Д. А. Погонышева, И. Г. Степченко. - 4-е изд., стер. - Москва : ФЛИНТА, 2022. - 184 с. - ISBN 978-5-9765-1904-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1875457 (дата обращения: 06.03.2025). – Режим доступа: по подписке.
2.	Козьминых, С. И. Организационное и правовое обеспечение информационной безопасности : учебное пособие / С. И. Козьминых. - Тбилиси : Справедливая Грузия, 2020. - 309 с. - ISBN 978-9941-9663-2-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1359091 (дата обращения: 06.03.2025). – Режим доступа: по подписке.

6.1.3. Периодические издания

Не предусмотрены.

6.1.4. Методические указания для обучающихся по освоению дисциплины

Методические указания находятся в стадии разработки

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» (далее - сеть «Интернет»), необходимых для освоения дисциплины

№ п/п	Название интернет-ресурса, адрес и режим доступа
1.	Википедия – свободная энциклопедия. [Электронный ресурс]. URL: https://ru.wikipedia.org/ (дата обращения: 06.03.2025)
2.	Научная электронная библиотека «e-Library». [Электронный ресурс]. URL: https://elibrary.ru/ (дата обращения: 06.03.2025).
3.	Электронно-библиотечная система «Znanium» [Электронный ресурс]. URL: https://znanium.ru/ (дата обращения: 06.03.2025).
4.	Официальный сайт Совета безопасности URL:http://www.scrf.gov.ru/ (дата обращения: 06.03.2025).
5.	Портал по информационной безопасности URL: http://www.infosecurity.ru/ (дата обращения: 06.03.2025).
6.	информационно-аналитический портал сообщества менеджеров и экспертов в области информационной безопасности URL:http://защита-информации.su/ (дата обращения: 06.03.2025).
7.	Национальный форум информационной безопасности «ИНФОФОРУМ» — электронное периодическое издание по вопросам информационной безопасности URL: https://infoforum.ru/ (дата обращения: 06.03.2025).
8.	Anti-Malware.ru — независимый информационно-аналитический портал по информационной безопасности URL: https://www.anti-malware.ru/ (дата обращения: 06.03.2025).

6.3. Средства обеспечения освоения дисциплины

6.3.1. Компьютерные обучающие и контролирующие программы

№ п/п	Вид учебного занятия	Наименование программного обеспечения	Функция программного обеспечения		
			контроль	моделиру-ющая	обучающая
1	Лекционные, практические занятия, самостоятельная работа	http://moodle.lgau.ru	+	+	+

6.3.2. Аудио- и видеопособия
Не предусмотрены.

6.3.3. Компьютерные презентации учебных курсов
Не предусмотрены.

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

№ п/п	Наименование оборудованных учебных кабинетов, объектов для проведения занятий	Перечень основного оборудования, приборов и материалов
1.	Г-109 – аудитория для проведения, лекционных, семинарских лабораторных и практических занятий, групповых и индивидуальных консультаций, текущего контроля, промежуточной аттестации, самостоятельной работы, учебной практики, подготовки и проведение государственной итоговой аттестации	Компьютеры – 10 шт., рециркулятор – 1 шт., мультимедийный проектор - 1 шт., экран – 1 шт., стул мягкий – 1 шт., доска для тех.пок. – 1 шт., стол компьют. – 10 шт., стол аудиторный – 10 шт., стул ученич. – 30 шт.

8. Междисциплинарные связи

Протокол
согласования рабочей программы с другими дисциплинами

Наименование дисциплины, с которой проводилось согласование	Кафедра, с которой проводилось согласование	Предложения об изменениях в рабочей программе. Заключение об итогах согласования

Приложение 1

Лист изменений рабочей программы

Номер изменения	Номер протокола заседания кафедры и дата	Страницы с изменениями	Перечень откоррек-тированных пунктов	Подпись заве-дующего кафедрой

Приложение 2

Лист периодических проверок рабочей программы

Должностное лицо, проводившее проверку Ф.И.О., должность,	Дата	Потребность в корректировке	Перечень пунктов, стр., разделов, требующих изменений

Приложение 3

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ЛУГАНСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ ИМЕНИ К.Е. ВОРОШИЛОВА»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

учебной дисциплины «Информационная безопасность»

Направление подготовки: 38.03.05 Бизнес-информатика

Профиль: Бизнес-информатика

Уровень профессионального образования: бакалавр

Год начала подготовки: 2025

Луганск, 2025

7. **ПЕРЕЧЕНЬ КОМПЕТЕНЦИЙ, СООТНЕСЕННЫХ С ИНДИКАТОРАМИ ДОСТИЖЕНИЯ КОМПЕТЕНЦИЙ, С УКАЗАНИЕМ ЭТАПОВ ИХ ФОРМИРОВАНИЯ В ПРОЦЕССЕ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ**

Код контро-лируемой компе-тенции	Формулировка контролируемой компетенции	Индикаторы достижения компетенции	Этап (уровень) освоения компетенции	Планируемые результаты обучения	Наименование модулей и (или) разделов дисциплины	Наименование оценочного средства	
						Текущий контроль	Промежуточная аттестация
ПК-1	Способен формировать возможные решения на основе разработанных для них целевых показателей с учетом имеющихся факторов, условий и рисков и анализа требований заинтересованных сторон с точки зрения выбранных критериев	**ПК–1.1.** Осуществляет выявление, сбор, систематизацию, хранение, поддержание в актуальном состоянии, анализ, определение зависимости между элементами информации бизнес-анализа для формирования возможных решений используя современные методы исследования и применяя информационные технологии	Первый этап (пороговый уровень)	**Знать:** назначение и функции информационных технологий и современных программных продуктов для решения профессиональных задач	1. Теоретические основы информационной безопасности 2. Государственная система информационной безопасности. Законодательство в области информационной безопасности 3. Риски и угрозы информационной безопасности 4. Организационное обеспечение информационной безопасности 5. Технические средства и методы защиты информации 6. Средства антивирусной защиты информации 7. Средства восстановления данных 8. Политика	Тесты закрытого типа	Зачет/Экзамен
			Второй этап (продвинутый уровень)	**Уметь:** определять назначение и функции информационных систем и технологий для решения профессиональных задач		Тесты открытого типа (вопросы для опроса)	Зачет/Экзамен
			Третий этап (высокий уровень)	**Иметь навыки:** работы с информационными системами и технологиями для решения профессиональных задач		Практические задания	Зачет/Экзамен
		ПК-1.4. Составляет описание	Первый этап (пороговый уровень)	**Знать:** информационные технологии и		Тесты закрытого типа	Зачет/Экзамен

		возможных решений в соответствии с выбранными подходами с учетом имеющихся факторов, условий и рисков		программные средства для решения профессиональных задач	информационной безопасности организации (предприятия) 9. Электронный документооборот, основные понятия и требования безопасности 10. Теоретические и организационные основы систем электронного документооборота организации 11. Экономические аспекты информационной безопасности 12. Информационная безопасность в социально-экономических системах		
			Второй этап (продвинутый уровень)	**Уметь:** применять информационные технологии и программные средства для решения профессиональных задач		Тесты открытого типа (вопросы для опроса)	Зачет/Экзамен
			Третий этап (высокий уровень)	**Иметь навыки:** применения информационные технологии и программные средства для решения профессиональных задач		Практические задания	Зачет/Экзамен
ПК-2	Способен проводить анализ, обоснование и выбор решения с использованием информационны	**ПК-2.1.** Проводит анализ решений и оценку ресурсов, необходимых	Первый этап (пороговый уровень)	**Знать:** методы сбора, анализа, систематизации информации о факторах внешней и внутренней среды предприятия	1. Теоретические основы информационной безопасности 2. Государственная система информационной	Тесты закрытого типа	Зачет/Экзамен

	х технологий и современных методов исследования	для реализации решения с точки зрения достижения целевых показателей решений	Второй этап (продвинутый уровень)	**Уметь:** анализировать внутренние (внешние) факторы и условия, влияющие на деятельность организации	безопасности. Законодательство в области информационной безопасности 3. Риски и угрозы информационной безопасности 4. Организационное обеспечение информационной безопасности 5. Технические средства и методы защиты информации 6. Средства антивирусной защиты информации 7. Средства восстановления данных 8. Политика информационной безопасности организации (предприятия) 9. Электронный документооборот, основные понятия и требования безопасности 10. Теоретические и организационные основы систем электронного	Тесты открытого типа (вопросы для опроса)	Зачет/Экзамен
			Третий этап (высокий уровень)	**Иметь навыки:** разработки этапов принятия управленческих решений рациональным методом; анализа факторов, влияющих на процесс принятия решений		Практические задания	Зачет/Экзамен

					документооборота организации 11. Экономические аспекты информационной безопасности 12. Информационная безопасность в социально-экономических системах		
		ПК-2.3. Применяет информационные технологии (программные средства и платформы) инфраструктуры информационных технологий организаций, используя современные подходы и стандарты автоматизации, в объеме, необходимом для целей	Первый этап (пороговый уровень)	**Знать:** цели и задачи стратегических изменений в организации, основные параметры и ключевые показатели эффективности разрабатываемых стратегических изменений в организации	1. Теоретические основы информационной безопасности 2. Государственная система информационной безопасности. Законодательство в области информационной безопасности 3. Риски и угрозы информационной безопасности 4. Организационное обеспечение информационной безопасности 5. Технические средства и методы	Тесты закрытого типа	Зачет/Экзамен
			Второй этап (продвинутый уровень)	**Уметь:** проводить оценку вариантов разрабатываемых стратегий с точки зрения выбранных критериев		Тесты открытого типа (вопросы для опроса)	Зачет/Экзамен

		бизнес анализа и адаптации бизнес-процессов заказчика к возможностям информационной системы	Третий этап (высокий уровень)	**Иметь навыки:** оценки эффективности реализации стратегии по результатам деятельности предприятия с точки зрения реализации выбранных целей	защиты информации 6. Средства антивирусной защиты информации 7. Средства восстановления данных 8. Политика информационной безопасности организации (предприятия) 9. Электронный документооборот, основные понятия и требования безопасности 10. Теоретические и организационные основы систем электронного документооборота организации 11. Экономические аспекты информационной безопасности 12. Информационная безопасность в социально-экономических системах	Практические задания	Зачет/Экзамен

2. ОПИСАНИЕ ПОКАЗАТЕЛЕЙ И КРИТЕРИЕВ ОЦЕНИВАНИЯ КОМПЕТЕНЦИЯ НА РАЗЛИЧНЫХ ЭТАПАХ ИХ ФОРМИРОВАНИЯ, ОПИСАНИЕ ШКАЛ ОЦЕНИВАНИЯ

№ п/п	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде	Критерии оценивания	Шкала оценивания
1.	**Тест**	Система стандартизированных заданий, позволяющая измерить уровень знаний.	Тестовые задания	В тесте выполнено 90-100% заданий	Оценка «*Отлично*» (5)
				В тесте выполнено более 75-89% заданий	Оценка «*Хорошо*» (4)
				В тесте выполнено 60-74% заданий	Оценка «*Удовлетворительно*» (3)
				В тесте выполнено менее 60% заданий	Оценка «*Неудовлетворительно*» (2)
				Большая часть определений не представлена, либо представлена с грубыми ошибками.	Оценка «*Неудовлетворительно*» (2)
2.	**Опрос**	Форма работы, которая позволяет оценить кругозор, умение логически построить ответ, умение продемонстрировать монологическую речь и иные коммуникативные навыки. Устный опрос обладает большими возможностями воспитательного воздействия, создавая условия для неформального общения.	Вопросы к опросу	Продемонстрированы предполагаемые ответы; правильно использован алгоритм обоснований во время рассуждений; есть логика рассуждений.	Оценка «*Отлично*» (5)
				Продемонстрированы предполагаемые ответы; есть логика рассуждений, но неточно использован алгоритм обоснований во время рассуждений и не все ответы полные.	Оценка «*Хорошо*» (4)
				Продемонстрированы предполагаемые ответы, но неправильно использован алгоритм обоснований во время рассуждений; отсутствует логика рассуждений; ответы не полные.	Оценка «*Удовлетворительно*» (3)
				Ответы не представлены.	Оценка «*Неудовлетворительно*» (2)
3.	**Практические задания**	Направлено на овладение методами и методиками изучаемой дисциплины. Для решения предлагается решить конкретное задание (ситуацию) без применения математических расчетов.	Практические задания	Продемонстрировано свободное владение профессионально-понятийным аппаратом, владение методами и методиками дисциплины. Показаны способности самостоятельного мышления, творческой активности. Задание выполнено в полном объеме.	Оценка «*Отлично*» (5)
				Продемонстрировано владение профессионально-понятийным аппаратом, при применении	Оценка «*Хорошо*» (4)

№ п/п	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде	Критерии оценивания	Шкала оценивания
				методов и методик дисциплины незначительные неточности, показаны способности самостоятельного мышления, творческой активности. Задание выполнено в полном объеме, но с некоторыми неточностями.	
				Продемонстрировано владение профессионально-понятийным аппаратом на низком уровне; допускаются ошибки при применении методов и методик дисциплины. Задание выполнено не полностью.	Оценка «*Удовлетворительно*» (3)
				Не продемонстрировано владение профессионально-понятийным аппаратом, методами и методиками дисциплины. Задание не выполнено.	Оценка «*Неудовлетворительно*» (2)
4.1	**Зачет**	Зачет выставляется в результате подведения итогов текущего контроля. Зачет в форме итогового контроля проводится для обучающихся, которые не справились с частью заданий текущего контроля.	Вопросы к зачету	Показано знание теории вопроса, понятийного аппарата; умение содержательно излагать суть вопроса; владение навыками аргументации и анализа фактов, явлений, процессов в их взаимосвязи. Выставляется обучающемуся, который освоил не менее 60% программного материала дисциплины.	«Зачтено»
				Знание понятийного аппарата, теории вопроса, не продемонстрировано; умение анализировать учебный материал не продемонстрировано; владение аналитическим способом изложения вопроса и владение навыками аргументации не продемонстрировано. Обучающийся освоил менее 60% программного материала дисциплины.	«Не зачтено»

№ п/п	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде	Критерии оценивания	Шкала оценивания
4.2	**Экзамен**	Контрольное мероприятие, которое проводится по окончании изучения дисциплины.	Вопросы к экзамену	Показано знание теории вопроса, понятийно-терминологического аппарата дисциплины; умение анализировать проблему, содержательно и стилистически грамотно излагать суть вопроса; глубоко понимать материал; владение аналитическим способом изложения вопроса, научных идей; навыками аргументации и анализа фактов, событий, явлений, процессов. Выставляется обучающемуся, полно, подробно и грамотно ответившему на вопросы билета и вопросы экзаменатора.	Оценка «*Отлично*» (5)
				Показано знание основных теоретических положений вопроса; умение анализировать явления, факты, действия в рамках вопроса; содержательно и стилистически грамотно излагать суть вопроса, но имеет место недостаточная полнота ответов по излагаемому вопросу. Продемонстрировано владение аналитическим способом изложения вопроса и навыками аргументации. Выставляется обучающемуся, полностью ответившему на вопросы билета и вопросы экзаменатора, но допустив при ответах незначительные ошибки, указывающие на наличие несистемности и пробелов в знаниях.	Оценка «*Хорошо*» (4)
				Показано знание теории вопроса фрагментарно (неполнота изложения информации; оперирование понятиями на бытовом уровне); умение выделить главное, сформулировать выводы, показать связь в построении ответа не продемонстрировано. Владение аналитическим способом изложения вопроса и владение навыками аргументации не продемонстрировано. Обучающийся допустил несущественные ошибки при ответах на вопросы билетов и	Оценка «*Удовлетворительно*» (3)

№ п/п	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде	Критерии оценивания	Шкала оценивания
				вопросы экзаменатора.	
				Знание понятийного аппарата, теории вопроса, не продемонстрировано; умение анализировать учебный материал не продемонстрировано; владение аналитическим способом изложения вопроса и владение навыками аргументации не продемонстрировано. Обучающийся не ответил на один или два вопроса билета и дополнительные вопросы экзаменатора.	Оценка «*Неудовлетворительно*» (2)

3. ТИПОВЫЕ КОНТРОЛЬНЫЕ ЗАДАНИЯ ИЛИ ИНЫЕ МАТЕРИАЛЫ, НЕОБХОДИМЫЕ ДЛЯ ОЦЕНКИ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ И (ИЛИ) ОПЫТА ДЕЯТЕЛЬНОСТИ, ХАРАКТЕРИЗУЮЩИХ ЭТАПЫ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ В ПРОЦЕССЕ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Оценочные средства для проведения текущего контроля

Текущий контроль осуществляется преподавателем дисциплины при проведении занятий в форме тестовых заданий, устного опроса и практических заданий.

ПК-1. Способен формировать возможные решения на основе разработанных для них целевых показателей с учетом имеющихся факторов, условий и рисков и анализа требований заинтересованных сторон с точки зрения выбранных критериев.

ПК-1.1. Осуществляет выявление, сбор, систематизацию, хранение, поддержание в актуальном состоянии, анализ, определение зависимости между элементами информации бизнес-анализа для формирования возможных решений используя современные методы исследования и применяя информационные технологии.

Первый этап (пороговой уровень) – показывает сформированность показателя компетенции «знать»: назначение и функции информационных технологий и современных программных продуктов для решения профессиональных задач.

Тестовые задания закрытого типа

1. Сетевой протокол - это: (выберите один вариант ответа)
а) набор соглашений о взаимодействиях в компьютерной сети;
б) правила установления связи между двумя компьютерами в сети;
в) последовательная запись событий, происходящих в компьютерной сети;
г) правила интерпретации данных, передаваемых по сети

2. Топология – это … (выберите один вариант ответа)
а) среда передачи информации;
б) стандарт взаимодействия абонентов в сети;
в) совокупность средств для взаимодействия пользователя с сетью;
г) метод соединения, структура связей абонентов в сети

3. Какой протокол является базовым в Интернет? (выберите один вариант ответа)
а) HTTP
б) HTML
в) TCP
г) TCP/IP

4. Экспертные системы – это … (выберите один вариант ответа)
а) системы обработки базы знаний
б) системы обработки знаний в узкоспециализированной области подготовки решений пользователей на уровне профессиональных экспертов
в) системы для разработки ППП различных предметных областей
г) системы для автоматизации деятельности фирм, не связанных с материальным производством

5. Гипертекст – это… (выберите один вариант ответа)

а) очень большой текст
б) текст, набранный на компьютере
в) текст, в котором используется шрифт большого размера
г) структурированный текст, в котором могут осуществляться переходы

Ключи

1.	б
2.	г
3.	в
4.	б
5.	г

6. ***Прочитайте текст и установите соответствие***

В таблице приведены базовые понятия в области электронного документооборота и их определение. Установите между ними соответствие.

Формулировка	Понятие
1. Правительство, которое взаимодействует с органами государственной власти, гражданами и организациями в электронном формате с минимальным личным (физическим) взаимодействием.	а) электронный документ
2. Информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и используется для определения лица, подписывающего информацию.	б) электронный документооборот
3. Процесс, направленный на оцифровку всех информационных ресурсов (создание цифровых копий) и формирование сетевых платформ взаимодействия, с целью получения прогнозируемого и гарантированного результата на любое управляющее воздействие с использованием средств автоматизации.	в) электронная подпись
4. Составление и обмен документами в электронном виде по защищённым каналам без необходимости распечатывать их и физически подписывать.	г) цифровизация
5. Документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах	д) электронное правительство
	е) электронный архив

Запишите в таблицу выбранные буквы под соответствующими цифрами

1	2	3	4	5
д	в	г	б	а

Второй этап (продвинутый уровень) – показывает сформированность показателя компетенции «уметь»: определять назначение и функции информационных систем и технологий для решения профессиональных задач.

Задания закрытого типа (вопросы для опроса):

1. Дайте определение понятия «угроза конфиденциальности».

2. Что называют «вредоносным программным обеспечением»?

3. Перечислите виды ответственности за использование не лицензионного программного обеспечения.

4. Дайте определение понятия «идентификация».

5. Сервисное программное обеспечение. Дать определение, привести примеры.

Ключи

1.	Угроза конфиденциальности – нарушение свойства информации быть известной только определенным субъектам.
2.	Вредоносное ПО — это приложения или код, которые препятствуют нормальному использованию конечных устройств. Когда устройство заражено вредоносным ПО, вы можете столкнуться с несанкционированным доступом, компрометацией данных или блокировкой и требованием заплатить выкуп. Вредоносное ПО распространяют киберпреступники. Их цель — получить деньги, а также использовать зараженные устройства для новых атак.
3.	Использование нелицензионного программного обеспечения является нарушением авторских и смежных прав и влечет за собой административную (ст. 7.12. КоАП РФ), уголовную (ст. 146 УК РФ) и гражданско-правовую ответственность.
4.	Идентификация — это процесс, когда информационная система, например социальная сеть или интернет-магазин, определяет, существует конкретный пользователь или нет. Делает она это с помощью идентификатора. Идентификатором может быть логин, электронная почта, номер телефона или другой признак, который есть только у одного пользователя.
5.	Сервисное программное обеспечение — программы, которые нужны для технической работы с информацией: поддержания порядка на компьютере, защиты информации, уменьшения её объёма. Примеры сервисных программ: антивирусы; архиваторы; программы для обслуживания жёсткого диска.

Третий этап (высокий уровень) – показывает сформированность показателя компетенции «иметь навыки»: работы с информационными системами и технологиями для решения профессиональных задач.

Практические задания:

1. После переезда на новое место жительства вам для работы необходимо подключить интернет и организовать беспроводную сеть, путем подключения роутера. Какой протокол защиты Wi-Fi лучше выбрать?

2. . Какая технология разработана для упрощения подключения устройств к сетям Wi-Fi. С ее помощью можно подключиться к роутеру без пароля.

3. После работы за чужим компьютером папки на вашем USB-накопителе стали «невидимыми». Но по объему занимаемой информации видно, что данные папки есть на USB-накопителе. Как путем использования Total Commander сделать так, чтоб папки снова отображались при открытии USB-накопителя?

4. Торговое предприятие Retail продают товары через магазины, онлайн-платформы, рынки и другие каналы сбыта, доступные для граждан. Сектор включает в себя широкий спектр товаров и услуг. Как обезопасить имеющуюся на предприятии электронную базу данных от непредвиденной потери данных?

5. Для работы Вам необходимо найти определенное программное обеспечение, драйвера подключенных устройств. После установки скачанных приложений было

установлено дополнительно стороннее программное обеспечение, которое не получается удалить. Как вернуть вернуться к первоначальному состоянию системы?

Ключи

1.	WPA2
2.	технология WPS
3.	Изменить атрибуты папок
4.	Систематическое резервное копирование
5.	Использовать точку восстановления компьютера

ПК-1.4. Составляет описание возможных решений в соответствии с выбранными подходами с учетом имеющихся факторов, условий и рисков.

Первый этап (пороговой уровень) – показывает сформированность показателя компетенции «знать»: информационные технологии и программные средства для решения профессиональных задач.

Тестовые задания закрытого типа

1. Вредоносная программа, которая подменяет собой загрузку некоторых программ при загрузке системы, называется... (выберите один вариант ответа)
а) загрузочный вирус
б) макровирус
в) троян
г) файловый вирус

2. К биометрической системе защиты относятся (выберите один вариант ответа)
а) защита паролем
б) физическая защита данных
в) антивирусная защита
г) идентификация по отпечаткам пальцев

3. Что можно противопоставить взлому системы защиты информации? (выберите один вариант ответа)
а) систему контроля передаваемых сообщений
б) установку дополнительной системы защиты
в) введение специальных паролей
г) создание защищенного домена для системы защиты

4. Как решается проблема защиты каналов передачи данных между головным офисом и филиалами компании? (выберите один вариант ответа)
а) с помощью специального программного обеспечения
б) шифровкой передаваемых сообщений
в) с помощью защищенных частных сетей
г) передачей информации специальными курьерами

5. Что представляют собой средства мониторинга? (выберите один вариант ответа)
а) это набор утилит, отслеживающих операции с файлами, реестром, портами и сетью
б) это набор утилит, используемых для вывода на монитор текстовой информации
в) это набор утилит, защищающих информацию от вирусов
г) это набор утилит, позволяющих сократить время выполнения арифметических операций

Ключи

1.	а
2.	г
3.	г
4.	в
5.	а

6. ***Прочитайте текст и установите соответствие***

В таблице приведены основные методы защиты при доступе к информационной системе и их характеристики. Установите между ними соответствие.

Характеристика	Методы защиты
1. Метод идентификации пользователя в каком-либо сервисе при помощи запроса данных двух разных типов	а) идентификация
2. Предоставление определённых прав доступа и разрешений пользователю на использование ресурсов.	б) авторизация
3. Процесс проверки и подтверждения достоверности чего-либо с использованием различных методов	в) двухфакторная аутентификация
4. Оценка характеристик пользователя для определения его личности	г) аутентификация
5. Процесс идентификации пользователя или устройства, позволяющий установить его подлинность и право доступа к определённым ресурсам или функционалу системы	д) шифрование
	е) верификация

Запишите в таблицу выбранные буквы под соответствующими цифрами

1	2	3	4	5
в	б	е	а	г

Второй этап (продвинутый уровень) – показывает сформированность показателя компетенции «уметь»: применять информационные технологии и программные средства для решения профессиональных задач.

Задания открытого типа (вопросы для опроса):

1. В чем заключается сущность приема, обеспечивающего несанкционированный доступ к конфиденциальной информации и известного как «уборка мусора»?
2. Частью какой, более общей системы, является система обеспечения информационной безопасности Российской Федерации?
3. На кого распространяется действие Закона «О государственной тайне»?
4. Каким образом должен быть организован процесс формирования и потребления информации, составляющей коммерческую тайну предприятия?
5. Аутентификацией называют…

Ключи

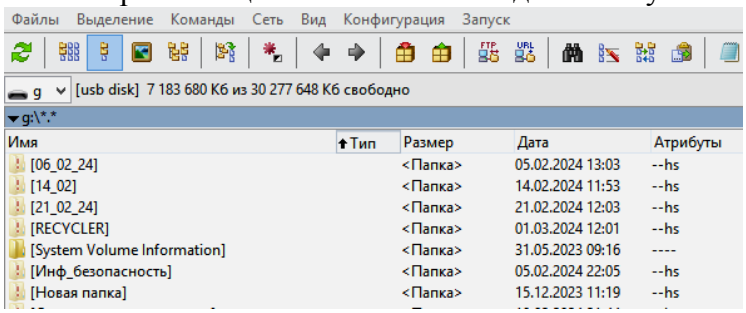
1.	метод получения информации, оставленной пользователем в памяти ПК после окончания работы
2.	системы обеспечения национальной безопасности страны
3.	на всех граждан и должностных лиц, если им предоставили для работы закрытые

	сведения
4.	он должен быть организован таким образом, чтобы исключить утечку информации
5.	процесс распознавания и проверки подлинности заявлений о себе пользователей и процессов

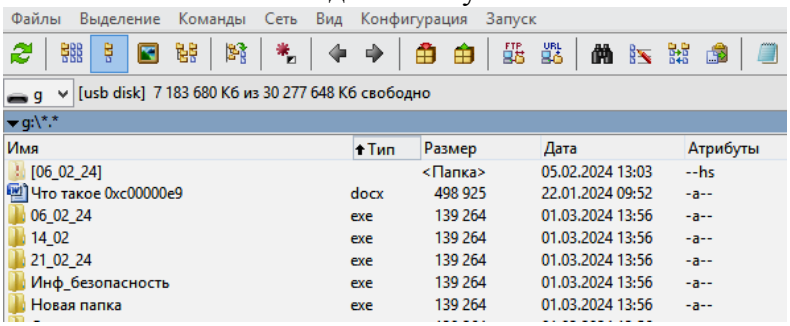
Третий этап (высокий уровень) – показывает сформированность показателя компетенции «иметь навыки»: применения информационные технологии и программные средства для решения профессиональных задач.

Практические задания:

1. При открытии накопителя часть папок имеют полупрозрачный вид с восклицательным знаком красного цвета. О чем это свидетельствует?



2. После работы за чужим компьютером часть папок и файлов исчезли и появились папки с расширением *.exe*. О чем это свидетельствует?



3. В зависимости от среды обитания вирусы можно разделить на сетевые, файловые и загрузочные. Сетевые вирусы распространяются по различным компьютерным сетям. Файловые вирусы внедряются главным образом в исполняемые модули. Куда внедряются загрузочные вирусы?

4. Запустить ping компьютера: «Пуск»->«Выполнить»->*“cmd”->“ping ip-addr -t”*. Где располагается утилита **ping**?

5. Методы обеспечения информационной безопасности Российской Федерации направленные на создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий, вызывающих разрушение, уничтожение, искажение информации, а также изменение штатных режимов функционирования систем и средств информатизации и связи.

Ключи

1.	папки являются скрытыми
2.	накопитель заражен вирусом
3.	в сектор загрузки системного диска (Master Boot Record)
4.	в системной папке Windows (C:\windows\system)
5.	организационно-технические методы

ПК-2. Способен проводить анализ, обоснование и выбор решения с использованием информационных технологий и современных методов исследования.

ПК-2.1. Проводит анализ решений и оценку ресурсов, необходимых для реализации решения с точки зрения достижения целевых показателей решений.

Первый этап (пороговой уровень) – показывает сформированность показателя компетенции «знать»: методы сбора, анализа, систематизации информации о факторах внешней и внутренней среды предприятия.

Тестовые задания закрытого типа

1. К правовым методам, обеспечивающим информационную безопасность, относятся… (выберите один вариант ответа)

а) разработка аппаратных средств обеспечения правовых данных;

б) разработка и установка во всех компьютерных правовых сетях журналов учета действий;

в) разработка и конкретизация правовых нормативных актов обеспечения безопасности;

г) обязательная идентификация при входе в информационную систему.

2. Конфиденциальностью называется… (выберите один вариант ответа)

а) описание процедур;

б) защита программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов;

в) защита от несанкционированного доступа к информации;

г) разграничение доступа.

3. Основными источниками угроз информационной безопасности являются… (выберите один вариант ответа)

а) хищение жестких дисков, подключение к сети, инсайдерство

б) Перехват данных, хищение данных, изменение архитектуры системы

в) Хищение данных, подкуп системных администраторов, нарушение регламента работы

г) все указанное в списке

4. Таргетированная атака – это…(выберите один вариант ответа)

а) атака на компьютерную систему крупного предприятия

б) атака на конкретный компьютер пользователя

в) атака на сетевое оборудование

г) атака на конкретную учетную запись

5. Основная масса угроз информационной безопасности приходится на… (выберите один вариант ответа)

а) Черви

б) Шпионские программы

в) Троянские программы

г) Макровирусы

Ключи

1.	в
2.	в
3.	б
4.	а
5.	в

6. ***Прочитайте текст и установите соответствие***
В таблице приведены основные виды компьютерных вирусов и их характеристики. Установите между ними соответствие.

Основные характеристики вируса	Виды компьютерных вирусов
1. Вирус способный копировать себя и распространяться с одного устройства на другое через сеть, заражая все попавшиеся на её путь устройства.	а) Загрузочный вирус
2. Разновидность компьютерных вирусов, разработанных на макроязыках, встроенных в такие прикладные пакеты программного обеспечения, как Microsoft Office.	б) Полиморфный вирус
3. Компьютерный вирус, записывающийся в первый сектор гибкого или жёсткого диска и выполняющийся при загрузке компьютера. Данный вирус может контролировать загрузку операционной системы и перехватывать управление перед передачей его операционной системе.	в) Сетевой вирус
4. Компьютерный вирус, прикрепляющий себя к файлу или программе и активизирующийся при каждом использовании файла. Для своего размножения использует файловую систему, внедряясь в исполняемые файлы практически любой операционной системы.	г) Макровирус
5. Вирус, полностью или частично скрывающий своё присутствие в системе путём перехвата обращений к операционной системе.	д) Файловый вирус
	е) Стелс-вирус

Запишите в таблицу выбранные буквы под соответствующими цифрами

1	2	3	4	5
в	г	а	д	е

Второй этап (продвинутый уровень) – показывает сформированность показателя компетенции «уметь»: анализировать внутренние (внешние) факторы и условия, влияющие на деятельность организации.

Задания открытого типа (вопросы для опроса):

1. Перечислите типы архивации и их возможности, которые можно выполнить с помощью элемента *Панель управления – Архивация и восстановление.*
2. Перечислите основные виды сетевых атак.
3. Перечислите основные каналы несанкционированного доступа.
4. Признаки заражения компьютера вирусами.
5. Раскройте понятие «фишинг».

Ключи

1.	Имеются три типа архивирования: 1. Системное архивирование - записывается архивный образ операционной системы 2. Полное архивирование - сохранение всех данных. 3. Нарастающее (инкрементальное) архивирование - записываются только изменения относительно последнего полного архивирования. Этот тип архивирования самый быстрый, но его необходимо проводить очень внимательно.
2.	Существует два основных типа сетевых атак: пассивные и активные. При пассивных

	сетевых атаках злоумышленники входят в сети без разрешения, контролируют и крадут личную информацию без внесения каких-либо изменений. Активные сетевые атаки включают изменение, шифрование или повреждение данных.
3.	Основные каналы несанкционированного доступа к информации могут включать: – установление контакта с лицами, имеющими или имевшими доступ к конфиденциальной информации; – вербовка и внедрение агентов; – физическое проникновение к носителям конфиденциальной информации; – подключение к средствам отображения, хранения, обработки, воспроизведения и передачи информации, средства связи; – прослушивание речевой конфиденциальной информации; – визуальный съём конфиденциальной информации; – перехват электромагнитных излучений.
4.	Некоторые признаки заражения компьютера вирусами: – снижение производительности (медленная работа и долгий запуск программ) – проблемы с жёстким диском (например, длительная запись или копирование данных) – всплывающие окна – проблемы с доступом к учётным записям (внезапная потеря доступа к учётной записи по старому паролю или уведомления о попытке смены пароля) – некорректная работа браузера – появление новых и незнакомых программ, файлов, ярлыков – долгое выключение или перезагрузка компьютера.
5.	Фишинг (от англ. fishing — рыбачить, выуживать) — вид кибератаки, при которой злоумышленник пытается получить доступ к личной информации пользователя. Например, к логину и паролю от электронной почты или данным банковской карты.

Третий этап (высокий уровень) – показывает сформированность показателя компетенции «иметь навыки»: разработки этапов принятия управленческих решений рациональным методом; анализа факторов, влияющих на процесс принятия решений.

Практические задания:

1. Для передачи сообщения используется код, состоящий из прописных латинских букв и цифр (всего используется 30 различных символов). При этом все символы кодируются одним и тем же (минимально возможным) количеством битов. Определите информационный объём сообщения длиной в 100 символов.
2. Метеорологическая станция ведет наблюдение за влажностью воздуха. Результатом одного наблюдения является целое число от 0 до 100%, записываемое при помощи минимально возможного количества бит. Станция сделала 300 измерений. Определите информационный объем результатов наблюдений.
3. Максимальная скорость передачи данных в локальной сети 100 Мбит/с. Сколько страниц текста можно передать за 1 сек, если 1 страница текста содержит 50 строк и на каждой строке - 70 символов?
4. Для передачи сообщения используется код, состоящий из прописных латинских букв (всего используется 20 различных символов). При этом все символы кодируются одним и тем же (минимально возможным) количеством битов. Определите информационный объём сообщения длиной в 200 символов.
5. В течение двух минут производилась четырёхканальная звукозапись с частотой дискретизации 16 КГц и 32-битным разрешением без сжатия. В ответе укажите целое количество мегабайт, необходимых для хранения такой аудиозаписи.

Ключи

1.	62,5 байта
2.	262,5 байта
3.	3571,43 страниц
4.	125 байт
5.	30 Мб

ПК-2.3. Применяет информационные технологии (программные средства и платформы) инфраструктуры информационных технологий организаций, используя современные подходы и стандарты автоматизации, в объеме, необходимом для целей бизнес анализа и адаптации бизнес- процессов заказчика к возможностям информационной системы.

Первый этап (пороговой уровень) – показывает сформированность показателя компетенции «знать»: цели и задачи стратегических изменений в организации, основные параметры и ключевые показатели эффективности разрабатываемых стратегических изменений в организации.

Тестовые задания закрытого типа

1. Какие основные функции выполняют электронные системы управления документооборотом? (выберите один вариант ответа)

а) создание электронных запросов
б) отслеживание и регистрация документов
в) подготовка отчетов
г) автоматизация процессов обработки и передачи документов

2. Какой принципиальный элемент присутствует в системах управления документооборотом для обеспечения безопасности данных? (выберите один вариант ответа)

а) учетная книга
б) база данных сотрудников
в) электронная подпись
г) печать

3. Что означает термин «Workflow» в контексте электронных систем управления документооборотом? (выберите один вариант ответа)

а) назначение электронного документа
б) графическое изображение печати организации
в) последовательность этапов обработки документа
г) секретный код для доступа к базе данных

4. Что такое «Электронная подпись» в системах управления документооборотом? (выберите один вариант ответа)

а) изображение на экране компьютера
б) закладка в электронном документе
в) электронный код, подтверждающий авторство и подлинность документа
г) секретный код для доступа к компьютеру

5. Какие типы документов могут обрабатываться в системах управления документооборотом? (выберите один вариант ответа)

а) Только текстовые документы
б) Скан-копии бумажных документов

в) Различные форматы, включая текстовые, графические и электронные документы
г) Только фотографии

Ключи

1.	г
2.	в
3.	в
4.	в
5.	в

6. ***Прочитайте текст и установите соответствие***
В таблице приведены базовые понятия в области электронного документооборота и их определение. Установите между ними соответствие.

Основные понятия	Формулировка
1. Информационная система структурированного защищенного хранения документов в оцифрованном виде.	а) внутренний документооборот
2. Обмен документами между организацией и внешними контрагентами: партнёрами, клиентами, поставщиками.	б) система электронного документооборота
3. Движение документов в организации с момента создания или получения до отправки или списания в дело	в) квалифицированная электронная подпись
4. Усовершенствованная электронная подпись с квалифицированным цифровым сертификатом, созданная устройством для создания квалифицированной подписи	г) внешний документооборот
5. Сервис, с помощью которого организовывается работа с документами внутри компании.	д) электронный архив
	е) внутренний документооборот

Запишите в таблицу выбранные буквы под соответствующими цифрами

1	2	3	4	5
д	г	а	в	б

Второй этап (продвинутый уровень) – показывает сформированность показателя компетенции «уметь»: проводить оценку вариантов разрабатываемых стратегий с точки зрения выбранных критериев.

Задания закрытого типа (вопросы для опроса):

1. Перечислите основные этапы документооборота.
2. Дайте определение понятию «*Интранет (Intranet)».*
3. CASE-технология разработки информационных систем.
4. Главные угрозы для систем электронного документооборота.
5. Приведите примеры государственных информационных ресурсов (ИР).

Ключи

1.	1) Составление и оформление документов. 2) Прием и регистрация документов. 3) Контроль за исполнением документов. 4) Передача документов в архив. Каждый из вышеуказанных этапов может быть выполнен как в традиционном, так и автоматизированном режиме.
2.	Интранет (Intranet) – компьютерная сеть для обмена информацией, инструментами совместной работы, операционными системами и другими вычислительными услугами внутри организации, обычно без доступа посторонних.

3.	Средства автоматизации разработки программ (CASE-средства) — инструменты автоматизации процессов проектирования и разработки программного обеспечения для системного аналитика, разработчика ПО и программиста.
4.	1) Угроза целостности – искажение или уничтожение информации (как случайное, так и намеренное). 2) Угроза конфиденциальности – кража информации, ее перехват. 3) Угроза функционированию системы – различные угрозы, вследствие которых происходят сбои в работе системы: преднамеренные атаки, ошибки пользователей, сбои в работе оборудования и программном обеспечения.
5.	Библиотечная сеть; архивный фонд; государственная система статистики; государственная система НТИ; государственная система правовой информации; ИР органов государственной власти и местного самоуправления; ИР о природных ресурсах и явлениях, процессах; ИР социальной сферы; ИР в сфере финансов и внешнеэкономической деятельности.

Третий этап (высокий уровень) – показывает сформированность показателя компетенции «иметь навыки»: оценки эффективности реализации стратегии по результатам деятельности предприятия с точки зрения реализации выбранных целей.

Практические задания:

1. Писатель на сайте издательства хочет внести правки в свою еще не изданную книгу, которая доступна для редактирования еще несколько недель. После того, как правки будут внесены для их сохранения, писатель должен воспользоваться *ЭП* данного вида.
2. Обязательно ли использование сертифицированных носителей (токенов) для ключа электронной подписи и какой закон регулирует данный вопрос? Какие сертификаты может иметь сертифицированный токен?
3. Женщина обратилась к нотариусу онлайн и заказала доверенность. Нотариус выполнил свою работу и в конце поставил на электронный документ перед его отправкой эту электронную подпись.
4. В новой компании «Х» реализовали систему электронного документооборота. На предприятии есть разные уровни доступа к документам, зависящие от должности сотрудников, поэтому должна быть обеспечена целостность документов в СЭДО (то есть необходимо обеспечить возможность обнаружения внесения изменений в документ). Какой вид ЭП стоит использовать для работы в организованной СЭДО?
5. В цифровом городе М, где все предприятия и госучреждения переведены на системы электронного документооборота, Типография №1 имеет соглашение с налоговой инспекцией, в котором описываются условия по предоставлению услуг печати налоговых бланков типографией. Для того, чтобы можно было свободно обмениваться теми или иными документами между сторонами (например отчетностью), необходимо наличие этого. Какой вид *ЭП* следует использовать для организации электронного документооборота между типографией и налоговой инспекцией?

Ключи

1.	Усиленная неквалифицированная ЭП
2.	Токены компании имеют, в зависимости от типа, сертификаты ФСТЭК и ФСБ, что подтверждает безопасность и соответствие криптографических алгоритмов требованиям стандартов в сфере безопасности.
3.	Усиленная квалифицированная ЭП
4.	Усиленная квалифицированная или неквалифицированная подпись
5.	Квалифицированная электронная подпись

Оценочные средства для проведения промежуточной аттестации

Промежуточная аттестация в 6 семестре проводится в форме зачета.

Вопросы для зачета

1. Теоретические аспекты информационной безопасности.
2. Составляющие информационной безопасности.
3. Доступность информации.
4. Целостность информации.
5. Конфиденциальность информации.
6. Правовое обеспечение информационной безопасности.
7. Доктрина информационной безопасности Российской Федерации.
8. Концепция информационной безопасности сетей связи общего пользования Российской Федерации.
9. Правовое обеспечение информационной безопасности в Российской Федерации.
10. Основные понятия организационного обеспечения информационной безопасности.
11. Административный уровень информационной безопасности.
12. Программа безопасности.
13. Уровни детализации политики информационной безопасности.
14. Технические средства и методы защиты информации.
15. Оценка безопасности информационных систем. Структура системы информационной безопасности.
16. Аппаратные средства защиты информации.
17. Вспомогательные аппаратные средства защиты информации.
18. Основные и вспомогательные программные средства защиты информации.
19. Ответственность за неправомерный доступ к компьютерной информации.
20. Определение понятия «коммерческая тайна» и «информация, составляющая коммерческую тайну».
21. Основные принципы обработки персональных данных.
22. Общая структура правового режима информационной безопасности.
23. Нормы и институты правового обеспечения информационной безопасности.
24. Система нормативно-правовых актов в области информационной безопасности в РФ.
25. Задачи защиты информации, определенные в ФЗ «Об информации, информационных технологиях и о защите информации».
26. Понятие «политика информационной безопасности».
27. Средства восстановления данных.
28. Средства резервного копирования, восстановления, защиты данных в операционных системах Windows.
29. Средства антивирусной защиты информации.
30. Источники вирусов. Признаки заражения и антивирусные программы.

Промежуточная аттестация в 7 семестре проводится в форме экзамена.

Вопросы для экзамена:

1. Основные определения и понятия в области информационной безопасности.
2. Показатели информации: важность, полнота, адекватность, релевантность, толерантность.
3. Доступность информации в контексте информационной безопасности.

4. Целостность информации в контексте информационной безопасности.
5. Конфиденциальность информации в контексте информационной безопасности.
6. Система защиты конфиденциальной информации.
7. Экономическая информация как товар и объект информационной безопасности.
8. Задачи информационной безопасности общества.
9. Комплексность системы защиты информации: инструментальная, структурная, функциональная, временная.
10. Правовое обеспечение информационной безопасности в Российской Федерации.
11. Доктрина информационной безопасности Российской Федерации.
12. Концепция информационной безопасности сетей связи общего пользования Российской Федерации.
13. Основные понятия организационного обеспечения информационной безопасности.
14. Информационные угрозы: понятие, виды и причины.
15. Предпосылки появления угроз.
16. Основные направления и методы реализации угроз.
17. Характер происхождения угроз (умышленные и естественные факторы).
18. Технологии (методики) управления информационными рисками.
19. Роль государства в минимизации рисков и угроз информационной безопасности.
20. Административный уровень информационной безопасности.
21. Структура системы информационной безопасности.
22. Уровни детализации политики информационной безопасности.
23. Технические средства и методы защиты информации.
24. Оценка безопасности информационных систем. Структура системы информационной безопасности.
25. Аппаратные средства защиты информации.
26. Вспомогательные аппаратные средства защиты информации.
27. Основные и вспомогательные программные средства защиты информации.
28. Ответственность за неправомерный доступ к компьютерной информации.
29. Определение понятия «коммерческая тайна» и «информация, составляющая коммерческую тайну».
30. Понятие «персональные данные. Классификация персональных данных.
31. Принципы обработки персональных данных.
32. Электронный документооборот, основные понятия и требования безопасности.
33. Юридическая сила электронного документа.
34. Электронная цифровая подпись и особенности ее применения.
35. Требования к системам электронного документооборота.
36. Структура, задачи и функции информационной системы электронного документооборота.
37. Критерии выбора программного обеспечения для системы электронного документооборота.
38. Структура правового режима информационной безопасности.
39. Нормы и институты правового обеспечения информационной безопасности.
40. Система нормативно-правовых актов в области информационной безопасности в РФ.
41. Задачи защиты информации, определенные в ФЗ «Об информации, информационных технологиях и о защите информации».
42. Понятие «политика информационной безопасности».
43. Средства восстановления данных.
44. Средства резервного копирования, восстановления, защиты данных.
45. Средства антивирусной защиты информации.
46. Источники вирусов. Признаки заражения и антивирусные программы.
47. Критерии выбора антивирусного программного обеспечения.

48. Экономические факторы и их роль в обеспечении информационной безопасности.
49. Методики оценки экономической эффективности системы обеспечения информационной безопасности.
50. Управление рисками информационной безопасности.
51. Экономические последствия нарушений информационной безопасности.
52. 1. Информационная безопасность электронной коммерции.
53. Уровни информационной безопасности.
54. Влияние цифровизации на национальную безопасность.
55. Информационная безопасность в финансовой сфере.
56. Особенности обеспечения информационной безопасности в сфере экономики.
57. Особенности обеспечения информационной безопасности в сфере науки и техники.
58. Особенности обеспечения информационной безопасности в сфере информационных и телекоммуникационных систем.
59. Основные положения государственной политики обеспечения информационной безопасности Российской Федерации.
60. Международное сотрудничество в сфере обеспечения информационной безопасности.

4. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРЫ ОЦЕНИВАНИЯ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ И (ИЛИ) ОПЫТА ДЕЯТЕЛЬНОСТИ

Для выполнения практических заданий студенту необходимы: ручка, листы для черновых подсчетов.

Текущий контроль

Тестирование для проведения текущего контроля проводится в виде тестов или системы дистанционного обучения Moodle.

На тестирование отводится 20 минут. Каждый вариант тестовых заданий включает 10 вопросов. Количество возможных вариантов ответов – 4. Студенту необходимо выбрать один правильный ответ. За каждый правильный ответ на вопрос присваивается 10 баллов. Шкала перевода: 9-10 правильных ответов – оценка «отлично» (5), 7-8 правильных ответов – оценка «хорошо» (4), 6 правильных ответов – оценка «удовлетворительно» (3), 1-5 правильных ответов – оценка «не удовлетворительно» (2).

Опрос как средство текущего контроля проводится в форме устных ответов на вопросы. Студент отвечает на поставленный вопрос сразу, время на подготовку к ответу не предоставляется.

Практические задания как средство текущего контроля проводятся в письменной форме. Студенту выдается задание и предоставляется 10 минут для подготовки к ответу.

Промежуточная аттестация

Зачет проводится путем подведения итогов по результатам текущего контроля. Если студент не справился с частью заданий текущего контроля, ему предоставляется возможность сдать зачет на итоговом контрольном мероприятии в форме ответов на вопросы к зачету или тестовых заданий к зачету, в случае дистанционного обучения.

Если зачет проводится в форме ответов на вопросы, студенту предлагается один или несколько вопросов из перечня вопросов к зачету. Время на подготовку к ответу не предоставляется.

Если зачет проводится в форме тестовых заданий к зачету, и тестирование для проведения текущего контроля проводится с помощью Системы дистанционного обучения Moodle, то на тестирование отводится 20 минут. Каждый вариант тестовых заданий включает 10 вопросов. Количество возможных вариантов ответов – 4. Студенту необходимо выбрать один правильный ответ. За каждый правильный ответ на вопрос присваивается 10 баллов. Шкала перевода: 9-10 правильных ответов – оценка «отлично» (5), 7-8 правильных ответов – оценка «хорошо» (4), 6 правильных ответов – оценка «удовлетворительно» (3), 1-5 правильных ответов – оценка «не удовлетворительно» (2).

Экзамен проводится в устной форме. Из экзаменационных вопросов составляется 20 экзаменационных билетов. Каждый билет состоит из трех теоретических вопросов. Комплект экзаменационных билетов представлен в учебно-методическом комплексе дисциплины.

На подготовку к ответу студенту предоставляется 20 минут.