Министерство сельского хозяйства Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ ИМЕНИ ИМПЕРАТОРА ПЕТРА I»

«УТВЕРЖДАЮ»
И.о. декана экономического факультета

Черных А.Н._____
«27» июня 2023 г.

РАБОЧАЯ ПРОГРАММА ПО ДИСЦИПЛИНЕ
Б1.В.12 Информационная безопасность

Специальность 38.05.01 Экономическая безопасность
Специализация «Экономико-правовое обеспечение экономической безопасности»

Квалификация выпускника экономист

Факультет Экономический

Кафедра Информационного обеспечения и моделирования агроэкономических систем

Разработчик(и) рабочей программы:

к. э. н., доцент Е.Ю. Горюхина

ДОКУМЕНТ ПОДПИСАН
Сертификат: 5454D669F460C778C21B8814FF5825E2
Владелец: Агибалов Александр Владимирович
Действителен: с 02.04.2024 до 26.06.2025

Рабочая программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по специальности 38.05.01 Экономическая безопасность (уровень специалитета), утвержденного приказом Министерства образования и науки Российской Федерации от 14 апреля 2021 г. № 293.

Рабочая программа утверждена на заседании кафедры Информационного обеспечения и моделирования агроэкономических систем протокол № 12 от 20.06.2023 г.

И.о. заведующего кафедрой **А.Н. Черных**

Рабочая программа рекомендована к использованию в учебном процессе методической комиссией экономического факультета протокол № 10 от 21.06.2023 г.

Председатель методической комиссии **/ Сальникова Е.Б.**

Рецензент: Директор ООО «ПАРТНЕР» Щербатых М.А.

1. Общая характеристика дисциплины

1.1. Цель дисциплины

Сформировать теоретические знания и умения для проведения анализа информационных угроз для предприятий и организаций, обеспечения комплексной защиты информационных ресурсов и управления информационными рисками.

1.2. Задачи дисциплины

Основные задачи дисциплины:

- формирование знаний основ в области информационной безопасности;
- формирование знаний о методах анализа и оценки состояния информационной безопасности в организации;
- формирование знаний о методах и средствах комплексной защиты информации в информационных системах коммерческих предприятий и государственных учреждений;
- формирование знаний и умений использования нормативно-правовых актов по вопросам информационной безопасности;
- формирование знаний, умений и навыков использования методов информационной безопасности в профессиональной деятельности.

1.3. Предмет дисциплины

Теоретические и практические аспекты обеспечения информационной безопасности предприятий и организаций АПК.

1.4. Место дисциплины в образовательной программе

Данная дисциплина является дисциплиной вариативного блока дисциплин.

1.5. Взаимосвязь с другими дисциплинами

Изучение данной дисциплины связано с изучением дисциплин: Б1.О.13 Экономическая безопасность, Б1.В.01 Безопасность электронного документооборота, Б1.В.10 Современные платежные системы и их безопасность

2. Планируемые результаты обучения по дисциплине

Дисциплина нацелена на формирование следующих компетенций:

Компетенция		Индикатор достижения компетенции	
код	**содержание**	**код**	**содержание**
ПК-3	Способен составлять прогнозы динамики основных экономических показателей деятельности хозяйствующих субъектов с учетом возможных экономических рисков и угроз экономической безопасности	З.6	**Знать** основные виды угроз информационной безопасности организаций
		У.6	**Уметь** проводить исследования в целях определения потенциальных и реальных угроз информационной безопасности организации
		Н.5	**Иметь навыки** осуществления мероприятий, направленных на определение потенциальных и реальных угроз информационной безопасности организации

3. Объём дисциплины и виды работ

3.1. Очная форма обучения

Показатели	Семестр	Всего
	3	
Общая трудоёмкость, з.е./ч	3 / 108	3 / 108
Общая контактная работа, ч	58.25	58.25
Общая самостоятельная работа, ч	49.75	49.75
Контактная работа при проведении учебных занятий, в т.ч. (ч)	58.00	58.00
лекции	30	30.00
практические	28	28.00
Самостоятельная работа при проведении учебных занятий, ч	40.90	40.90
Контактная работа при проведении промежуточной аттестации обучающихся, в т.ч. (ч)	0.25	0.25
зачет с оценкой	0.25	0.25
Самостоятельная работа при промежуточной аттестации, в т.ч. (ч)	8.85	8.85
подготовка к зачету с оценкой	8.85	8.85
Форма промежуточной аттестации	зачет с оценкой	зачет с оценкой

3.2. Заочная форма обучения

Показатели	Курс	Всего
	2	
Общая трудоёмкость, з.е./ч	3 / 108	3 / 108
Общая контактная работа, ч	12.25	12.25
Общая самостоятельная работа, ч	95.75	95.75
Контактная работа при проведении учебных занятий, в т.ч. (ч)	12.00	12.00
лекции	6	6.00
практические	6	6.00
Самостоятельная работа при проведении учебных занятий, ч	86.90	86.90
Контактная работа при проведении промежуточной аттестации обучающихся, в т.ч. (ч)	0.25	0.25
зачет с оценкой	0.25	0.25
Самостоятельная работа при промежуточной аттестации, в т.ч. (ч)	8.85	8.85
подготовка к зачету с оценкой	8.85	8.85
Форма промежуточной аттестации	зачет с оценкой	зачет с оценкой

4. Содержание дисциплины

4.1. Содержание дисциплины в разрезе разделов и подразделов

Раздел 1. Информационная безопасность

1.1. Основные понятия и термины в области информационной безопасности

1.2. Основные составляющие информационной безопасности: выявление субъектов информационных отношений и их интересов; категории безопасности: обеспечение доступности, целостности и конфиденциальности ресурсов информационной среды и поддерживающей инфраструктуры

1.3. Понятие и сущность защиты информации: предупреждение угроз; выявление угроз; обнаружение угроз; пресечение и локализация угроз; ликвидация угроз; ликвидация последствий угроз; общие признаки защиты информации

1.4. Предмет и объект защиты информации: характеристики качества информации; подходы к градации ценности информации; подходы объективной оценки количества информации; совокупность носителей информации, которая представляет собой комплекс физических, аппаратных, программных и документальных средств.

Раздел 2. Угрозы информационной безопасности

2.1. Понятие и классификация угроз информационной безопасности.

2.2. Случайные угрозы. Преднамеренные угрозы : стихийные бедствия и аварии; сбои и отказы; ошибки при разработке ИС; традиционный или универсальный шпионаж и диверсии; несанкционированный доступ к информации; электромагнитные излучения и наводки; модификация структур информационных систем; вредительские программы

2.3. Модель гипотетического нарушителя информационной безопасности

Раздел 3. Компьютерные преступления и их особенности

3.1. Понятие компьютерных преступлений и их виды: преступления, связанные с вмешательством в работу компьютера; преступления, использующие компьютер как необходимые технические средства

3.2. Вредоносное программное обеспечение: компьютерные вирусы, их классификация, признаки; программные закладки и их виды, механизмы их проникновения и действия, классификация, модели их воздействия; троянские программы, их задачи и воздействия, основные разновидности.

3.3. Методы и технологии борьбы с вредоносными программами: методы обнаружения, антивирусные программы, их функции, функциональные группы.

Раздел 4. Законодательные аспекты информационной безопасности в РФ

4.1. Законодательство РФ области информационной безопасности: основополагающие документы, предмет правового регулирования.

4.2. Нормативно-правовые основы информационной безопасности в РФ: основные положения ФЗ РФ № 5485-1 от 21.06.1993 г, основные положения ФЗ РФ № 149 от 27.08.2006 г., основные положения ФЗ РФ № 152 от 27.07.2006 г.

4.3 Ответственность за нарушения в сфере информационной безопасности в РФ: статьи 138, 140, 183, 237, 272, 273, 274, 283, 284 УК РФ.

Раздел 5. Криптографические методы защиты информации

5.1 Основные понятия и определения криптографии. История развития криптографии

5.2 Классификация криптографических методов защиты информации: виды преобразования (шифрование, кодирование), способы преобразования (подстановка, перестановка, аналитическое преобразование, гаммирование, комбинированные), разновидности криптографических преобразований, современные симметричные криптосистемы, асимметричные криптосистемы

5.3 Электронная подпись: назначение, возможности, преимущества, ФЗ РФ № 63 от 1.07.2013г., виды ЭП (простая, усиленная неквалифицированная, усиленная квалифицированная), OID, удостоверяющие центры и их функции.

Раздел 6. Системное обеспечение защиты информации

6.1 Концептуальная модель информационной безопасности: уровни ИБ, основные компоненты концептуальной модели ИБ, политика безопасности и её основные положения, оценка рисков и основные этапы разработки политики безопасности, группы процедурных мер ИБ, механизмы программно-технического уровня ИБ.

6.2 Основные принципы построения системы защиты: системность, комплексность, непрерывность, разумность и достаточность, гибкость управления и применения, простота применения мер и средств.

6.3 Методы защиты информации: минимизация ущерба от аварий и бедствий, повышение надежности ИС, защита от несанкционированного доступа.

Раздел 7. Информационная безопасность в условиях цифровой экономики

7.1 Особенности обеспечения информационной безопасности как элемента нац. программы «ЦЭ РФ»

7.2 Задачи и основополагающие принципы информационной безопасности в условиях цифровой экономики

7.3 Инструменты обеспечения информационной безопасности в условиях цифровой экономики

4.2. Распределение контактной и самостоятельной работы при подготовке к занятиям по подразделам

4.2.1. Очная форма обучения

Разделы, подразделы дисциплины	Контактная работа		СР
	лекции	ПЗ	
Раздел 1. Информационная безопасность			
Основные понятия и определения в области информационной безопасности	1		2
Основные составляющие информационной безопасности	1	1	2
Понятие и сущность защиты информации	1	1	2
Предмет и объект защиты информации	2		2
Раздел 2. Угрозы информационной безопасности			
Понятие и классификация угроз информационной безопасности	1		2
Случайные угрозы. Преднамеренные угрозы	1	1	2
Модель гипотетического нарушителя информационной безопасности	1	1	2
Раздел 3. Компьютерные преступления и их особенности			
Понятие компьютерных преступлений и их виды	2	1	3
Вредоносное программное обеспечение	2	1	3
Методы и технологии борьбы с вредоносными программами	2	2	3
Раздел 4. Законодательные аспекты информационной безопасности в РФ			
Законодательство РФ области информационной безопасности	2	1	3
Нормативно-правовые основы информационной безопасности в РФ	2	1	3
Ответственность за нарушения в сфере информационной безопасности в РФ	1	2	3
Раздел 5. Криптографические методы защиты информации			
Основные понятия, определения и история развития криптографии.	1		2
Классификация криптографических методов защиты информации	2	5	3
Электронная подпись	2	1	3
Раздел 6. Системное обеспечение защиты информации			
Концептуальная модель информационной безопасности	1		2
Основные принципы построения системы защиты	1		2
Методы защиты информации	2	8	3,9
Раздел 7. Информационная безопасность в условиях цифровой экономики			
Особенности обеспечения информационной безопасности как элемен-	0,5		1

та нац. программы «ЦЭ РФ»			
Задачи и основополагающие принципы информационной безопасности в условиях цифровой экономики	0,5		1
Инструменты обеспечения информационной безопасности в условиях цифровой экономики	1	2	1

4.2.2. Заочная форма обучения

Разделы, подразделы дисциплины	Контактная работа		СР
	лекции	ПЗ	
Раздел 1. Информационная безопасность			
Основные понятия и определения в области информационной безопасности	0,25		4
Основные составляющие информационной безопасности	0,25	0,5	4
Понятие и сущность защиты информации	0,25	0,5	4
Предмет и объект защиты информации	0,25		4
Раздел 2. Угрозы информационной безопасности			
Понятие и классификация угроз информационной безопасности	0,3		5
Случайные угрозы. Преднамеренные угрозы	0,3	0,5	5
Модель гипотетического нарушителя информационной безопасности	0,4	0,5	5
Раздел 3. Компьютерные преступления и их особенности			
Понятие компьютерных преступлений и их виды	0,3	0,3	5
Вредоносное программное обеспечение	0,3	0,3	5
Методы и технологии борьбы с вредоносными программами	0,4	0,4	5
Раздел 4. Законодательные аспекты информационной безопасности в РФ			
Законодательство РФ области информационной безопасности	0,3	0,3	5
Нормативно-правовые основы информационной безопасности в РФ	0,4	0,4	5
Ответственность за нарушения в сфере информационной безопасности в РФ	0,3	0,3	5
Раздел 5. Криптографические методы защиты информации			
Основные понятия, определения и история развития криптографии.	0,2		5
Классификация криптографических методов защиты информации	0,4	0,5	5
Электронная подпись	0,4	0,5	5
Раздел 6. Системное обеспечение защиты информации			
Концептуальная модель информационной безопасности	0,2		5
Основные принципы построения системы защиты	0,3		5
Методы защиты информации	0,5	0,5	5,9
Раздел 7. Информационная безопасность в условиях цифровой экономики			
Особенности обеспечения информационной безопасности как элемента нац. программы «ЦЭ РФ»			1
Задачи и основополагающие принципы информационной безопасности в условиях цифровой экономики			1
Инструменты обеспечения информационной безопасности в условиях цифровой экономики		0,5	3

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

Разделы, подразделы дисциплины	Учебно-методическое обеспечение	Объем часов СР	
		очная	заочная
Раздел 1. Информационная безопасность			
Основные понятия и определения в области информационной безопасности	Гришина Н.В. Основы информационной безопасности предприятия: учебное пособие/ Н.В. Гришина. - М: ИНФРА-М, 2021. - 216 с. - (Высшее образование: Специалитет). - URL: https://znanium.com/catalog/product/1178150 Горюхина Е.Ю. Информационная безопасность: Учебное пособие: для студентов, обучающихся по специальности 38.05.01 «Экономическая безопасность» / Е.Ю. Горюхина, Л.И. Литвинова, Н.В. Ткачева.- Воронеж : ВГАУ, 2015 .- 221 с. Горюхина Е.Ю. Информационная безопасность: Практикум для аудиторных занятий для студентов, обучающихся по специальности 38.05.01 «Экономическая безопасность» / Е. Ю. Горюхина, И. М. Семенова, Е. П. Суворова - Воронеж: ВГАУ, 2015. - 93 с.	2	4
Основные составляющие информационной безопасности		2	4
Понятие и сущность защиты информации		2	4
Предмет и объект защиты информации		2	4
Раздел 2. Угрозы информационной безопасности			
Понятие и классификация угроз информационной безопасности	Гришина Н.В. Основы информационной безопасности предприятия: учебное пособие/ Н.В. Гришина. - М: ИНФРА-М, 2021. - 216 с. - (Высшее образование: Специалитет). - URL: https://znanium.com/catalog/product/1178150 Горюхина Е.Ю. Информационная безопасность: Практикум для аудиторных занятий для студентов, обучающихся по специальности 38.05.01 «Экономическая безопасность» / Е. Ю. Горюхина, И. М. Семенова, Е. П. Суворова - Воронеж: ВГАУ, 2015. - 93 с. Ищейнов В.Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации: учебное пособие / В.Я. Ищейнов, М.В. Мецатунян. - М: ИНФРА-М, 2022. - 256 с. - (Высшее образование: Специалитет). - URL: https://znanium.com/catalog/product/1861659	2	5
Случайные угрозы. Преднамеренные угрозы		2	5
Модель гипотетического нарушителя информационной безопасности		2	5
Раздел 3. Компьютерные преступления и их особенности			
Понятие компьютерных преступлений и их виды	Горюхина Е.Ю. Информационная безопасность: Учебное пособие: для студентов, обучающихся по специальности 38.05.01 «Экономическая безопасность» / Е.Ю. Горюхина, Л.И. Литвинова, Н.В. Ткачева - Воронеж: ВГАУ, 2015.- 221 с. Горюхина Е.Ю. Информационная безопасность: Практикум для аудиторных занятий для студентов, обучающихся по специальности 38.05.01 «Экономическая безопасность» / Е. Ю. Горюхина, И. М. Семенова, Е. П. Суворова - Воронеж: ВГАУ, 2015. - 93 с. Рычаго М.Е. Основы защиты информации: учебное пособие/ М.Е. Рычаго, И.В. Ершова, Р. Н. Тихомиров. - Владимир: ВЮИ ФСИН России, 2017. - 68 с. - URL: https://znanium.com/catalog/product/1864501	3	5
Вредоносное программное обеспечение		3	5
Методы и технологии борьбы с вредоносными программами		3	5
Раздел 4. Законодательные аспекты информационной безопасности в РФ			
Законодательство РФ области информационной безопасности	Гришина Н.В. Основы информационной безопасности предприятия: учебное пособие/ Н.В. Гришина. - М: ИНФРА-М, 2021. - 216 с. - (Высшее образование: Специалитет). - URL: https://znanium.com/catalog/product/1178150	3	5

Нормативно-правовые основы информационной безопасности в РФ	Горюхина Е.Ю. Информационная безопасность: Учебное пособие: для студентов, обучающихся по специальности 38.05.01 «Экономическая безопасность» / Е.Ю. Горюхина, Л.И. Литвинова, Н.В. Ткачева - Воронеж: ВГАУ, 2015.- 221 с. Горюхина Е.Ю. Информационная безопасность: Практикум для аудиторных занятий для студентов, обучающихся по специальности 38.05.01 «Экономическая безопасность» / Е. Ю. Горюхина, И. М. Семенова, Е. П. Суворова - Воронеж: ВГАУ, 2015. - 93 с.	3	5
Ответственность за нарушения в сфере информационной безопасности в РФ		3	5
Раздел 5. Криптографические методы защиты информации			
Основные понятия, определения и история развития криптографии.	Баранова Е.К. Информационная безопасность. История специальных методов криптографической деятельности: учебное пособие / Е.К. Баранова, А.В. Бабаш, Д.А. Ларин. - М: РИОР : ИНФРА-М, 2022. - 236 с. - URL: https://znanium.com/catalog/product/1843171 Информационный мир XXI века. Криптография — основа информационной безопасности: методическое руководство / под ред. Э.А. Болелова; Московский государственный технический университет гражданской авиации. - 4-е изд. - М: Издательско-торговая корпорация «Дашков и К°», 2020. - 126 с. - URL: https://znanium.com/catalog/product/1081675 Горюхина Е.Ю. Информационная безопасность: Учебное пособие: для студентов, обучающихся по специальности 38.05.01 «Экономическая безопасность» / Е.Ю. Горюхина, Л.И. Литвинова, Н.В. Ткачева - Воронеж: ВГАУ, 2015.- 221 с. Горюхина Е.Ю. Информационная безопасность: Практикум для аудиторных занятий для студентов, обучающихся по специальности 38.05.01 «Экономическая безопасность» / Е. Ю. Горюхина, И. М. Семенова, Е. П. Суворова - Воронеж: ВГАУ, 2015. - 93 с.	2	5
Классификация криптографических методов защиты информации		3	5
Электронная подпись		3	5
Раздел 6. Системное обеспечение защиты информации			
Концептуальная модель информационной безопасности	Ищейнов В.Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации: учебное пособие / В.Я. Ищейнов, М.В. Мецатунян. - М: ИНФРА-М, 2022. - 256 с. - (Высшее образование: Специалитет). - URL: https://znanium.com/catalog/product/1861659 Горюхина Е.Ю. Информационная безопасность: Учебное пособие: для студентов, обучающихся по специальности 38.05.01 «Экономическая безопасность» / Е.Ю. Горюхина, Л.И. Литвинова, Н.В. Ткачева - Воронеж : ВГАУ, 2015 .- 221 с. Горюхина Е.Ю. Информационная безопасность: Практикум для аудиторных занятий для студентов, обучающихся по специальности 38.05.01 «Экономическая безопасность» / Е. Ю. Горюхина, И. М. Семенова, Е. П. Суворова - Воронеж: ВГАУ, 2015. - 93 с.	2	5
Основные принципы построения системы защиты		2	5
Методы защиты информации		3,9	5,9
Раздел 7. Информационная безопасность в условиях цифровой экономики			
Особенности обеспечения информационной безопасности как элемента нац. программы «ЦЭ РФ»	Горюхина Е.Ю. Информационная безопасность: Учебное пособие: для студентов, обучающихся по специальности 38.05.01 «Экономическая безопасность» / Е.Ю. Горюхина, Л.И. Литвинова, Н.В. Ткачева - Воронеж: ВГАУ, 2015.- 221 с. Гринев В.П. Цифровая экономика и правовое регулирование обеспечения ее информационной безопасности/ В.П. Гринев; под редакцией И. А. Цинделиани. - Москва: Проспект, 2021. - 384 с. - URL: https://e.lanbook.com/book/227222	1	1
Задачи и основополагающие принципы информационной безопасности в условиях цифровой экономики		1	1
Инструменты обеспечения информационной безопасности в условиях цифровой экономики		1	3

5. Фонд оценочных средств для проведения промежуточной аттестации

5.1. Этапы формирования компетенций

Разделы, подразделы дисциплины	**Компетенция**	**Индикатор достижения компетенции**
Раздел 1. Информационная безопасность		
Основные понятия и определения в области информационной безопасности	ПК-3	З.6
Основные составляющие информационной безопасности	ПК-3	З.6, У.6
Понятие и сущность защиты информации	ПК-3	З.6, У.6
Предмет и объект защиты информации	ПК-3	З.6
Раздел 2. Угрозы информационной безопасности		
Понятие и классификация угроз информационной безопасности	ПК-3	З.6
Случайные угрозы. Преднамеренные угрозы	ПК-3	З.6, У.6, Н.5
Модель гипотетического нарушителя информационной безопасности	ПК-3	З.6, У.6
Раздел 3. Компьютерные преступления и их особенности		
Понятие компьютерных преступлений и их виды	ПК-3	З.6
Вредоносное программное обеспечение	ПК-3	З.6, У.6
Методы и технологии борьбы с вредоносными программами	ПК-3	З.6, У.6, Н.5
Раздел 4. Законодательные аспекты информационной безопасности в РФ		
Законодательство РФ области информационной безопасности	ПК-3	З.6, У.6
Нормативно-правовые основы информационной безопасности в РФ	ПК-3	З.6, У.6
Ответственность за нарушения в сфере информационной безопасности в РФ	ПК-3	З.6, У.6
Раздел 5. Криптографические методы защиты информации		
Основные понятия, определения и история развития криптографии	ПК-3	З.6
Классификация криптографических методов защиты информации	ПК-3	З.6, У.6
Электронная подпись	ПК-3	З.6, У.6
Раздел 6. Системное обеспечение защиты информации		
Концептуальная модель информационной безопасности	ПК-3	З.6
Основные принципы построения системы защиты	ПК-3	З.6
Методы защиты информации	ПК-3	З.6, У.6, Н.5
Раздел 7. Информационная безопасность в условиях цифровой экономики		
Особенности обеспечения информационной безопасности как элемента нац. программы «ЦЭ РФ»	ПК-3	З.6
Задачи и основополагающие принципы информационной безопасности в условиях цифровой экономики	ПК-3	З.6
Инструменты обеспечения информационной безопасности в условиях цифровой экономики	ПК-3	З.6, У.6, Н.5

5.2. Шкалы и критерии оценивания достижения компетенций

5.2.1. Шкалы оценивания достижения компетенций

Вид оценки	Оценки			
Академическая оценка по 4-х балльной шкале	неудовлетворительно	удовлетворительно	хорошо	отлично

5.2.2. Критерии оценивания достижения компетенций

Критерии оценки на зачете с оценкой

Оценка, уровень достижения компетенций	Описание критериев
Отлично, высокий	Студент показал полные и глубокие знания программного материала, логично и аргументировано ответил на все вопросы экзаменационного билета, а также на дополнительные вопросы, способен самостоятельно решать сложные задачи дисциплины
Хорошо, продвинутый	Студент твердо знает программный материал, грамотно его излагает, не допускает существенных неточностей в ответе, достаточно полно ответил на вопросы экзаменационного билета и дополнительные вопросы, способен самостоятельно решать стандартные задачи дисциплины
Удовлетворительно, пороговый	Студент показал знание только основ программного материала, усвоил его поверхностно, но не допускал грубых ошибок или неточностей, требует наводящих вопросов для правильного ответа, не ответил на дополнительные вопросы, способен решать стандартные задачи дисциплины с помощью преподавателя
Неудовлетворительно, компетенция не освоена	Студент не знает основ программного материала, допускает грубые ошибки в ответе, не способен решать стандартные задачи дисциплины даже с помощью преподавателя

Критерии оценки тестов

Оценка, уровень достижения компетенций	Описание критериев
Отлично, высокий	Содержание правильных ответов в тесте не менее 90%
Хорошо, продвинутый	Содержание правильных ответов в тесте не менее 75%
Удовлетворительно, пороговый	Содержание правильных ответов в тесте не менее 50%
Неудовлетворительно, компетенция не освоена	Содержание правильных ответов в тесте менее 50%

Критерии оценки устного опроса

Оценка, уровень достижения компетенций	Описание критериев
Зачтено, высокий	Студент демонстрирует уверенное знание материала, четко выражает свою точу зрения по рассматриваемому вопросу, приводя соответствующие примеры
Зачтено, продвинутый	Студент демонстрирует уверенное знание материала, но допускает отдельные погрешности в ответе
Зачтено, пороговый	Студент демонстрирует существенные пробелы в знаниях материала, допускает ошибки в ответах
Не зачтено, компетенция не освоена	Студент демонстрирует незнание материала, допускает грубые ошибки в ответах

Критерии оценки решения задач

Оценка, уровень достижения компетенций	Описание критериев
Зачтено, высокий	Студент уверенно знает методику и алгоритм решения задачи, не допускает ошибок при ее выполнении.
Зачтено, продвинутый	Студент в целом знает методику и алгоритм решения задачи, не допускает грубых ошибок при ее выполнении.
Зачтено, пороговый	Студент в целом знает методику и алгоритм решения задачи, допускает ошибок при ее выполнении, но способен исправить их при помощи преподавателя.
Не зачтено, компетенция не освоена	Студент не знает методику и алгоритм решения задачи, допускает грубые ошибки при ее выполнении, не способен исправить их при помощи преподавателя.

5.3. Материалы для оценки достижения компетенций

5.3.1. Оценочные материалы промежуточной аттестации

5.3.1.1. Вопросы к экзамену

Не предусмотрен

5.3.1.2. Задачи к зачету с оценкой

№	Содержание	Компетенция	ИДК
1.	Определите время перебора всех паролей, состоящих из 6 цифр	ПК-3	У.6
2.	Определите минимальную длину пароля, алфавит которого состоит из 10 символов, время перебора которого было не меньше 10 лет	ПК-3	У.6
3.	Определите время перебора всех паролей с указанными параметрами	ПК-3	У.6
4.	Определите минимальную длину пароля, алфавит которого состоит из n символов, время перебора которого было не меньше t лет. Скорость перебора s паролей в секунду	ПК-3	У.6
5.	Определите количество символов алфавита, пароль состоит из k символов, время перебора которого было не меньше t лет. Скорость перебора s паролей в секунду.	ПК-3	У.6
6.	Проверьте потенциальные места записей «троянских программ» в системном реестре ОС	ПК-3	Н.5
7.	На основании предоставленного перечня информационных активов (ИА) предприятия распределите информационные активы на: составляющие коммерческую тайну, персональные данные и открытые активы.	ПК-3	У.6
8.	Укажите в подготовленном перечне сведения, доступ к которым не может быть ограничен	ПК-3	Н.5
9.	Укажите как подразделяется информация ограниченного доступа в соответствии с ФЗ-149?	ПК-3	У.6
10.	Выделите информацию конфиденциального характера	ПК-3	Н.5
11.	Выделите информацию ограниченного доступа	ПК-3	Н.5
12.	Выделите основные организационные мероприятия по защите информации	ПК-3	Н.5
13.	Настройте параметры локальной политики безопасности ОС	ПК-3	Н.5
14.	Используя метод шифрования - "перестановка", зашифровать свои данные: фамилию, имя, отчество	ПК-3	У.6

15.	Используя метод шифрования - "замена", зашифровать свои данные: фамилию, имя, отчество	ПК-3	У.6
16.	Определите примерный перечень сведений, составляющих коммерческую (служебную) тайну предприятия	ПК-3	У.6
17.	Укажите последовательность действий в системе КриптоАРМ при выполнении подписания документа	ПК-3	Н.5
18.	Укажите последовательность действий в системе КриптоАРМ для выполнения открытия документа	ПК-3	Н.5

5.3.1.3. Вопросы к зачёту с оценкой

№	Содержание	Компетенция	ИДК
1	Основные понятия и определения в области информационной безопасности	ПК-3	З.6
2	Основные составляющие информационной безопасности	ПК-3	З.6
3	Задачи информационной безопасности	ПК-3	З.6
4	Понятие и сущность защиты информации	ПК-3	З.6
5	Цели защиты информации. Предмет защиты информации	ПК-3	З.6
6	Законодательство РФ в области информационной безопасности	ПК-3	З.6
7	Нормативно-правовая база защиты информации: основные законы РФ и указы Президента РФ	ПК-3	З.6
8	Информация как объект права собственности. Объект защиты информации	ПК-3	З.6
9	Случайные угрозы информационной безопасности	ПК-3	З.6
10	Преднамеренные угрозы информационной безопасности	ПК-3	З.6
11	Модель гипотетического нарушителя информационной безопасности	ПК-3	З.6
12	Анализ компьютерных преступлений	ПК-3	З.6
13	Несанкционированный доступ к информации и его цели	ПК-3	З.6
14	Компьютерные вирусы	ПК-3	З.6
15	Шпионские программные закладки	ПК-3	З.6
16	Основные принципы построения системы защиты информации	ПК-3	З.6
17	Методы защиты информации	ПК-3	З.6
18	Основные понятия и определения криптографии	ПК-3	З.6
19	История развития криптографии	ПК-3	З.6
20	Классификация криптографических методов защиты информации	ПК-3	З.6
21	Современные симметричные криптографические системы: системы с секретным ключом	ПК-3	З.6
22	Современные симметричные криптографические системы: стандарт шифрования DES	ПК-3	З.6
23	Современные симметричные криптографические системы: стандарт шифрования ГОСТ 28147	ПК-3	З.6
24	Асимметричные криптографические системы: системы с открытым ключом;	ПК-3	З.6
25	Асимметричные криптографические системы: стандарт шифрования RSA	ПК-3	З.6
26	Электронная цифровая подпись и механизмы её реализации	ПК-3	З.6
27	Критерии защищенности компьютерных систем	ПК-3	З.6
28	Концептуальная модель информационной безопасности	ПК-3	З.6
29	Основные принципы построения системы защиты информации	ПК-3	З.6
30	Методы защиты информации	ПК-3	З.6

5.3.1.4. Вопросы к зачёту

Не предусмотрен.

5.3.1.5. Перечень тем курсовых проектов

Не предусмотрен.

5.3.1.6. Вопросы к защите курсового проекта

Не предусмотрен.

5.3.2. Оценочные материалы текущего контроля

5.3.2.1. Вопросы тестов

№	Содержание	Компетенция	ИДК
1	Информация, несанкционированное копирование, хищение, разглашение (распространение, опубликование), модификация, уничтожение или использование которой может нанести существенный моральный или материальный ущерб ее собственнику или владельцу, а также третьей стороне, интересы которой данная информация затрагивает, называется	ПК-3	З.6
2	Укажите категории ценности информации с точки зрения информационной безопасности	ПК-3	У.6
3	Категория ценности информации, определяющая гарантию того, что источником информации является именно то лицо, которое заявлено как ее автор, называется	ПК-3	З.6
4	Аутентичность связана	ПК-3	З.6
5	Категория ценности информации, гарантирующая, что при необходимости можно доказать, что автором сообщения является именно заявленный человек, и не может являться никто другой, называется	ПК-3	З.6
6	Убытки, которые могут возникнуть вследствие внесения изменений в информацию, если факт модификации не был обнаружен, называются	ПК-3	З.6
7	Потенциальные убытки, которые понесет владелец информации, если к ней получат неавторизованный доступ сторонние лица, называются	ПК-3	З.6
8	Ущерб от полного или частичного разрушения информации называется	ПК-3	У.6
9	Укажите, что не является преднамеренным воздействием на информационную систему	ПК-3	У.6
10	Укажите, что не является причиной случайных воздействии на информационную систему	ПК-3	У.6
11	Укажите пути несанкционированной передачи информации	ПК-3	У.6
12	Укажите составляющие информационной безопасности	ПК-3	У.6
13	Конфиденциальность информации гарантирует	ПК-3	З.6
14	Потенциально возможное событие, процесс или явление, которые могут привести к уничтожению, утрате целостности, конфиденциальности или доступности информации называется	ПК-3	З.6
15	Защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб владельцам или пользователям информации называется	ПК-3	З.6
16	Комплекс средств и методов, направленных на предотвращение угроз информационной безопасности и устранение их последствий, называется	ПК-3	З.6
17	Укажите, что из перечисленного является задачей информационной	ПК-3	У.6

	безопасности		
18	Доступность информации гарантирует	ПК-3	З.6
19	Целостность информации гарантирует	ПК-3	З.6
20	Процесс распознавания пользователя автоматизированной системой, для чего предъявляется уникальное имя, называется	ПК-3	З.6
21	Процедура проверки подлинности, предназначенная для подтверждения истинности пользователя, предъявившего идентификатор, называется	ПК-3	З.6
22	Идентификация и аутентификации применяются	ПК-3	З.6
23	Присвоение субъектам идентификаторов и (или) сравнение предъявляемых идентификаторов с перечнем идентификаторов, владельцы которых допущены к информационной системе, называется	ПК-3	З.6
24	Результатом реализации угроз информационной безопасности может быть	ПК-3	З.6
25	Угроза перехвата данных может привести	ПК-3	З.6
26	Идентификация и аутентификация применяются	ПК-3	З.6
27	Подберите слово к данному определению: ??? - проверка принадлежности субъекту предъявленного им идентификатора и подтверждение его подлинности	ПК-3	З.6
28	Подберите слово к данному определению: ??? - присвоение субъектам личного идентификатора и сравнение его с заданным	ПК-3	З.6
29	Под информационной безопасностью (безопасностью информации) понимается	ПК-3	З.6
30	Что такое угроза?	ПК-3	З.6
31	Бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена – это	ПК-3	З.6
32	Умышленные или неосторожные действия с конфиденциальными сведениями, приведшие к ознакомлению с ними лиц, не допущенных к ним – это	ПК-3	З.6
33	Противоправное преднамеренное овладение конфиденциальной информацией лицом, не имеющим права доступа к охраняемым секретам – это:	ПК-3	З.6
34	В чем выражаются угрозы информационной безопасности?	ПК-3	З.6
35	Мероприятия по формированию осознанного отношения сотрудников к обеспечению информационной безопасности относятся к:	ПК-3	З.6
36	Накопление сведений об угрозах информационной безопасности и их аналитическая обработка относится к:	ПК-3	З.6
37	Действия, направленные на устранение действующей угрозы и конкретных преступных действий относятся к :	ПК-3	З.6
38	Действия по восстановлению состояния, предшествовавшего возникновению угрозы, относятся к:	ПК-3	З.6
39	Основными мероприятиями по защите от разглашения является:	ПК-3	З.6
40	Защита от утечки конфиденциальной информации сводится к:	ПК-3	З.6
41	Защита от несанкционированного доступа к конфиденциальной информации обеспечивается выполнением:	ПК-3	З.6
42	Определение состояния технической безопасности объекта относится к:	ПК-3	З.6
43	Какой из принципов нецелесообразно использовать при организации защиты информации:	ПК-3	З.6
44	Уголовно наказуемые общественно опасные действия, в которых машинная информация является объектом посягательства, называют:	ПК-3	З.6

45	Любая программа, написанная с целью нанесения ущерба или использования ресурсов атакуемого компьютера, называется:	ПК-3	З.6
46	Класс программ, способных к саморазмножению и самомодификации в работающей вычислительной среде и вызывающих нежелательные для пользователей действия, называется:	ПК-3	З.6
47	Укажите этапы жизненного цикла компьютерного вируса:	ПК-3	З.6
48	По среде обитания компьютерные вирусы подразделяют на:	ПК-3	З.6
49	Достаточно трудно обнаружимые вирусы, не имеющие сигнатур, то есть не содержащие ни одного постоянного участка кода, это:	ПК-3	З.6
50	Вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям:	ПК-3	З.6
51	??? – это вирусы, заражающие файлы некоторых систем обработки документов (MS Word, MS Excel), которые имеют встроенные макроязыки	ПК-3	З.6
52	??? маскируют свое присутствие путем перехвата обращений ОС к пораженным файлам, секторам и переадресуют ОС к незараженным участкам	ПК-3	З.6
53	??? - это компьютерные вирусы, которые распространяются в компьютерных сетях и не изменяют файлы или секторы на диска	ПК-3	З.6
54	Какой из вирусов при инфицировании компьютера оставляет в оперативной памяти свою часть, которая затем перехватывает обращения операционной системы к объектам заражения и внедряется в них?	ПК-3	З.6
55	Самошифрование и полиморфичность используются для:	ПК-3	З.6
56	Одним из наиболее эффективных способов борьбы с вирусами является:	ПК-3	З.6
57	??? - это программа, скрытно внедренная в защищенную систему и позволяющая злоумышленнику, путем модификации свойств системы защиты, осуществлять несанкционированный доступ к ресурсам системы	ПК-3	З.6
58	К деструктивным действиям, осуществляемым программными закладками, относятся:	ПК-3	З.6
59	Программа с известными ее пользователю функциями, в которую были внесены изменения, чтобы, помимо этих функций, она могла втайне от него выполнять некоторые другие (разрушительные) действия, называется:	ПК-3	З.6
60	??? – это компьютерная программа, которая выявляет, предотвращает и выполняет определенные действия, чтобы блокировать или удалять вредоносные программы:	ПК-3	З.6
61	Укажите методы обнаружения компьютерных вирусов:	ПК-3	З.6
62	??? - комплекс программных или аппаратных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами. Позволяет блокировать нежелательный сетевой трафик, обеспечивает невидимость ПК в сети с целью предотвращения кибер атак	ПК-3	З.6
63	Маски (сигнатуры) вирусов используются:	ПК-3	З.6
64	Укажите основные функции антивирусных программ:	ПК-3	З.6
65	Основополагающими документами по информационной безопасности в РФ являются	ПК-3	З.6

66	Укажите документ, гарантирующий тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (ст. 23, ч. 2); право свободно искать, получать, передавать, производить и распространять информацию любым законным способом (ст. 29, ч. 4); свободу массовой информации (ст. 29, ч. 5):	ПК-3	У.6
67	Укажите документ, определяющий важнейшие задачи обеспечения информационной безопасности РФ:	ПК-3	У.6
68	Укажите сведения, имеющие конфиденциальный характер:	ПК-3	У.6
69	Сколько категорий государственных информационных ресурсов определяет Закон РФ «Об информации, информационных технологиях и о защите информации» от 27.08.2006 г. № 149-ФЗ?	ПК-3	З.6
70	Документированная информация, правовой режим которой установлен специальными нормами действующего законодательства в области государственной, коммерческой, промышленной и другой общественной деятельности, называется:	ПК-3	З.6
71	Любая информация, с помощью которой можно однозначно идентифицировать физическое лицо, является	ПК-3	З.6
72	Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ, относятся к	ПК-3	З.6
73	Неправомерный доступ к компьютерной информации наказывается штрафом	ПК-3	З.6
74	Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети наказывается ограничением свободы на срок	ПК-3	З.6
75	Создание, использование и распространение вредоносных программ для ЭВМ наказывается:	ПК-3	З.6
76	Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети наказывается:	ПК-3	З.6
77	Что такое Доктрина информационной безопасности РФ	ПК-3	З.6
78	В предлагаемом перечне укажите мероприятия защиты информации предприятия, относящиеся к правовым?	ПК-3	У.6
79	Право разрешать или ограничивать доступ к информации и определять условия такого доступа принадлежит:	ПК-3	З.6
80	Перечень сведений конфиденциального характера определен:	ПК-3	З.6
81	Перечень сведений, доступ к которым не может быть ограничен определен:	ПК-3	З.6
82	Наука о методах преобразования информации с целью ее защиты от несанкционированного доступа называется	ПК-3	З.6
83	Наука (и практика ее применения) о методах и способах расшифрования информации без знания ключей называется	ПК-3	З.6
84	Набор средств и методов сокрытия факта передачи сообщения называется	ПК-3	З.6
85	Процесс преобразования исходного (открытого) сообщения в шифрованное по определенным правилам, содержащимся в шифре называется	ПК-3	З.6
86	Процесс преобразования шифрованного сообщения (шифртекста) в исходное (открытое) сообщение с помощью определенных правил, содержащихся в шифре называется	ПК-3	З.6
87	Способ преобразования информации с целью ее защиты от незаконных пользователей называется	ПК-3	З.6

88	Процесс получения защищенного сообщения (открытого текста) из шифрованного сообщения (шифротекста) без знания примененного шифра называется:	ПК-3	З.6
89	Сменный элемент шифра, применяемый для шифрования конкретных сообщений, называется	ПК-3	З.6
90	Укажите способы преобразования при шифровании	ПК-3	З.6
91	Криптосистемой является	ПК-3	З.6
92	Что из перечисленного не входит в криптосистему:	ПК-3	З.6
93	ГОСТ 28147-89 является стандартом	ПК-3	З.6
94	Алгоритм RSA является стандартом:	ПК-3	З.6
95	При асимметричном шифровании для шифрования и расшифровки используются:	ПК-3	З.6
96	Реквизит электронного документа, полученный в результате криптографического преобразования информации с использованием закрытого ключа, предназначенный для защиты данного документа от подделки, и позволяющий идентифицировать владельца ключа, а также установить отсутствие искажения информации в электронном документе, представляет собой	ПК-3	З.6
97	Цифровая подпись не обеспечивает	ПК-3	З.6
98	Соотнесите виды цифровой подписи и их характеристики	ПК-3	У.6
99	Алгоритмы шифрования бывают	ПК-3	З.6
100	Реквизит электронного документа, полученный в результате криптографического преобразования информации с использованием закрытого ключа и предназначенный для защиты данного документа от подделки, а также позволяющий идентифицировать владельца ключа и установить отсутствие искажения информации в электронном документе называется	ПК-3	З.6
101	Электронная подпись устанавливает ??? информации	ПК-3	З.6
102	Электронная подпись обеспечивает	ПК-3	З.6
103	Программные модули или аппаратные устройства, регистрирующие каждое нажатие клавиши на клавиатуре компьютера	ПК-3	З.6
104	Для генерации электронной подписи может быть использован алгоритм	ПК-3	З.6
105	Какие из перечисленных алгоритмов относятся к симметричным?	ПК-3	З.6
106	Для контроля целостности передаваемых по сетям данных используется	ПК-3	З.6
107	В предлагаемом перечне выделите задачи, не являющиеся задачами криптографии	ПК-3	У.6
108	Что из перечисленного не является функцией управления криптографическими ключами	ПК-3	З.6
109	Программная или программно-аппаратная система, которая выполняет контроль информационных потоков, поступающих в информационную систему и/или выходящих из нее, и обеспечивает защиту информационной системы посредством фильтрации информации называется	ПК-3	З.6
110	Электронная подпись позволяет	ПК-3	З.6
111	Размер ключа в ГОСТ 28147-89	ПК-3	З.6
112	Размер ключа в стандарте DES	ПК-3	З.6
113	Символы исходного текста складываются с символами некой случайной последовательности – это	ПК-3	З.6

114	Символы оригинального текста меняются местами по определенному принципу, являющемуся секретным ключом – это	ПК-3	З.6
115	Какой метод используется при шифровании с помощью аналитических преобразований	ПК-3	З.6
116	Сферы применения DES-алгоритма	ПК-3	З.6
117	Алгоритм ГОСТ 28147-89 использует ключ, являющийся	ПК-3	З.6
118	Основные области применения DES-алгоритма	ПК-3	З.6
119	Криптостойкость – это…	ПК-3	З.6
120	Что не рассматривается в политике безопасности?	ПК-3	З.6
121	Совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов, называется:	ПК-3	З.6
122	Стратегию организации в области информационной безопасности, меру внимания и количество ресурсов, которые руководство считает целесообразным выделить для обеспечения информационной безопасности, определяет:	ПК-3	З.6
123	Укажите компоненты концептуальной модели безопасности информации:	ПК-3	З.6
124	На каком из уровней обеспечения информационной безопасности разрабатывается политика безопасности:	ПК-3	З.6
125	Что не является содержанием административного уровня обеспечения информационной безопасности:	ПК-3	З.6
126	Какой из уровней обеспечения информационной безопасности включает комплекс мероприятий, реализующих практические механизмы защиты информации:	ПК-3	З.6
127	Какой из перечисленных уровней не относится к уровням обеспечения информационной безопасности:	ПК-3	З.6
128	Какие из указанных мероприятий защиты информации относятся к организационным?	ПК-3	З.6
129	Организационные мероприятия защиты информации реализуются на каких уровнях:	ПК-3	З.6
130	Какие из указанных мероприятий защиты информации относятся к инженерно-техническим?	ПК-3	З.6
131	Возможности несанкционированного использования конфиденциальных сведений в значительной мере обусловливаются:	ПК-3	З.6
132	Система защиты информации – это:	ПК-3	З.6
133	К недостаткам аппаратных средств инженерно-технической защиты относится:	ПК-3	З.6
134	К достоинствам программных средств инженерно-технической защиты относится:	ПК-3	З.6
135	Началу работ по созданию или совершенствованию системы защиты информации (СЗИ) предшествует:	ПК-3	З.6
136	Мероприятия по созданию системы защиты информации начинаются с:	ПК-3	З.6
137	Информационная модель предприятия формируется после окончания	ПК-3	З.6
138	Разработка системы защиты информации начинается с	ПК-3	З.6
139	Контроль эффективности защиты необходимо начинать с	ПК-3	З.6

5.3.2.2. Вопросы для устного опроса

№	Содержание	Компетенция	ИДК
1	Дайте определение понятию информационная безопасность.	ПК-3	З.6
2	Перечислите основные составляющие информационной безопасности.	ПК-3	З.6
3	Какое значение имеют составляющие информационной безопасности для субъектов информационных отношений?	ПК-3	З.6
4	Каковы интересы РФ в информационной сфере?	ПК-3	З.6
5	Определите источники угроз информационной безопасности РФ и постройте их классификацию.	ПК-3	З.6
6	Перечислите основные методы обеспечения информационной безопасности РФ.	ПК-3	З.6
7	Какие основные проблемы международного сотрудничества стоят на повестке дня сегодня?	ПК-3	З.6
8	На ваш взгляд, каково положение дел в области мировой информационной безопасности сегодня?	ПК-3	У.6
9	Проанализируйте различные определения понятия «защита информации» и «информационная безопасность»	ПК-3	З.6
10	Дайте определение понятию защита информации.	ПК-3	З.6
11	Что понимается под термином безопасность информации?	ПК-3	З.6
12	Что включает в себя защита информации?	ПК-3	З.6
13	Какие цели преследует защита информации?	ПК-3	З.6
14	Какое место занимает защита информации в информационной безопасности?	ПК-3	З.6
15	Определите предмет защиты информации.	ПК-3	З.6
16	Сформулируйте основные свойства информации.	ПК-3	З.6
17	Дайте определение конфиденциальной информации.	ПК-3	З.6
18	Перечислите уровни секретности государственной тайны.	ПК-3	З.6
19	Раскройте сущность основных подходов к измерению количества информации.	ПК-3	З.6
20	Раскройте сущность информации как объекта права собственности.	ПК-3	З.6
21	Раскройте сущность объекта защиты.	ПК-3	З.6
22	Определите понятие угрозы информационной безопасности (ИБ).	ПК-3	З.6
23	Укажите и охарактеризуйте случайные угрозы ИБ.	ПК-3	У.6
24	Укажите и охарактеризуйте преднамеренные угрозы ИБ.	ПК-3	У.6
25	Определите понятия нарушителя ИБ и злоумышленника.	ПК-3	З.6
26	Укажите какие предположения выдвигаются при разработке модели гипотетического нарушителя ИБ объекта.	ПК-3	У.6
27	На основании чего строится модель гипотетического нарушителя ИБ?	ПК-3	З.6
28	Какие категории персонала объекта могут быть внутренними нарушителями ИБ объекта?	ПК-3	З.6
29	Какие лица могут быть нарушителями ИБ объекта из числа посторонних лиц?	ПК-3	З.6
30	Укажите основные мотивы нарушений ИБ.	ПК-3	У.6
31	Дайте определение компьютерного преступления и охарактеризуйте их виды	ПК-3	З.6
32	Определите понятия вредоносного программного обеспечения и компьютерного вируса	ПК-3	З.6
33	Перечислите основные классы компьютерных вирусов	ПК-3	З.6
34	В чем заключаются различия между понятиями компьютерного виру-	ПК-3	З.6

	са и шпионской программной закладки?		
35	Укажите основные методы внедрения программных закладок	ПК-3	У.6
36	Дайте характеристику основных моделей воздействия программных закладок на компьютер и компьютерную сеть	ПК-3	У.6
37	В чем различия троянских программ и программных закладок?	ПК-3	З.6
38	Дайте характеристику действий основных разновидностей троянских программ	ПК-3	З.6
39	Назовите и охарактеризуйте методы обнаружения вирусов	ПК-3	З.6
40	Перечислите виды и назначения антивирусных программ	ПК-3	З.6
41	Какими действиями можно предотвратить вирусную атаку?	ПК-3	З.6
42	Укажите основополагающие документы по ИБ в РФ.	ПК-3	З.6
43	Что является предметом правового регулирования в области ИБ?	ПК-3	З.6
44	Назовите задачи обеспечения ИБ, сформулированные в Концепции национальной безопасности РФ	ПК-3	З.6
45	Какой закон является базовым в области защиты информации, и какие отношения он регламентирует?	ПК-3	З.6
46	Назовите категории государственных информационных ресурсов	ПК-3	З.6
47	Укажите какая информация может быть отнесена к категории конфиденциальной?	ПК-3	У.6
48	Определите данные, которые могут быть отнесены к персональным данным	ПК-3	У.6
49	Назовите статьи УК РФ, предусматривающие ответственность за совершение компьютерных преступлений	ПК-3	З.6
50	Сформулируйте основные принципы построения системы защиты информации.	ПК-3	У.6
51	Какие уровни задействованы в обеспечении информационной безопасности?	ПК-3	З.6
52	Что представляет собой политика безопасности организации?	ПК-3	З.6
53	Что входит в анализ рисков?	ПК-3	З.6
54	Что представляет собой программа безопасности организации?	ПК-3	З.6
55	Перечислите основные модели защиты информации и их особенности.	ПК-3	З.6
56	В чем заключается сущность методов защиты от случайных угроз?	ПК-3	З.6
57	Дайте определение понятиям идентификации и аутентификации.	ПК-3	З.6
58	Перечистите основные виды аутентификации.	ПК-3	З.6
59	В чем заключается повышение надежности и отказоустойчивости информационных систем?	ПК-3	З.6
60	Какую роль играет подготовленность персонала в построении системы защиты информации?	ПК-3	З.6
61	Какие методы и средства используются для организации противодействия традиционным методам шпионажа и диверсий?	ПК-3	З.6
62	Раскройте особенность построения защиты от несанкционированного доступа	ПК-3	У.6
63	Какие методы защиты информации относятся к криптографическим?	ПК-3	З.6
64	Дайте определение криптологии.	ПК-3	З.6
65	Какие три основных периода криптологии вы знаете?	ПК-3	З.6
66	Объясните понятие «криптологический алгоритм».	ПК-3	З.6
67	Что такое криптография?	ПК-3	З.6
68	Покажите на примерах суть преобразований перестановки и замены.	ПК-3	У.6
69	Что собой представляют шифрование и дешифрование?	ПК-3	З.6
70	Дайте определение аналитическому преобразованию, гаммированию	ПК-3	З.6

	и комбинированному шифрованию.		
71	Что такое системы с открытыми ключами?	ПК-3	З.6
72	Приведите структурную схему процесса шифрования с открытым ключом.	ПК-3	З.6
73	Дайте определение стойкости криптосистемы.	ПК-3	З.6
74	Приведите основные программно-аппаратные реализации шифров.	ПК-3	У.6
75	В чем заключается суть DES-алгоритма? Каковы его особенности?	ПК-3	З.6
76	В каких режимах может работать DES-алгоритм?	ПК-3	З.6
77	Дайте описание отечественного алгоритма криптографического преобразования данных (ГОСТ 28147 - 89) и его отличительных особенностей.	ПК-3	З.6
78	Какими характеристиками оценивается стойкость криптографических систем?	ПК-3	З.6
79	В чем заключается суть электронной цифровой подписи?	ПК-3	З.6
80	Как проверяется целостность сообщения?	ПК-3	У.6
81	Дайте определение межсетевого экрана.	ПК-3	З.6
82	Назовите типы межсетевых экранов.	ПК-3	З.6
83	Объясните различия между межсетевыми экранами разных типов.	ПК-3	З.6
84	Что представляет собой политика безопасности организации?	ПК-3	З.6
85	Что не рассматривается в политике безопасности?	ПК-3	З.6
86	Укажите компоненты концептуальной модели безопасности информации.	ПК-3	У.6
87	На каком из уровней обеспечения информационной безопасности разрабатывается политика безопасности?	ПК-3	З.6
88	Что является содержанием административного уровня обеспечения информационной безопасности?	ПК-3	З.6
89	Какой уровень обеспечения информационной безопасности включает комплекс мероприятий, реализующих практические механизмы защиты информации?	ПК-3	З.6
90	Назовите мероприятия защиты информации, являющиеся организационными?	ПК-3	З.6
91	На каких уровнях защиты информации реализуются организационные мероприятия?	ПК-3	З.6
92	Укажите какие мероприятия защиты информации относятся к классу инженерно-техническим?	ПК-3	З.6
93	Что понимается под системой защиты информации?	ПК-3	З.6
94	Что можно считать недостатками аппаратных средств инженерно-технической защиты информации?	ПК-3	З.6
95	Что можно считать достоинствами программных средств инженерно-технической защиты информации?	ПК-3	З.6
96	Что предшествует началу работ по созданию или совершенствованию системы защиты информации (СЗИ)?	ПК-3	З.6
97	С чего следует начинать мероприятия по созданию системы защиты информации?	ПК-3	З.6
98	На каком этапе осуществляется фомирование информационной модели предприятия?	ПК-3	З.6

5.3.2.3. Задачи для проверки умений и навыков

№	Содержание	Компетенция	ИДК
1	Определите время перебора всех паролей, состоящих из 6 цифр	ПК-3	У.6
2	Определите минимальную длину пароля, алфавит которого состоит из 10 символов, время перебора которого было не меньше 10 лет	ПК-3	У.6
3	Определите время перебора всех паролей с указанными параметрами	ПК-3	У.6
4	Определите минимальную длину пароля, алфавит которого состоит из n символов, время перебора которого было не меньше t лет. Скорость перебора s паролей в секунду	ПК-3	У.6
5	Определите количество символов алфавита, пароль состоит из k символов, время перебора которого было не меньше t лет. Скорость перебора s паролей в секунду.	ПК-3	У.6
6	Выполните архивацию файла с паролем. Внесите искажения, попытайтесь разархивировать. В отчете отразить: контрольную сумму исходного файла, сжатого файла, выдаваемые сообщения об ошибках при разархивировании искаженного файла.	ПК-3	У.6
7	Выполните архивацию файла с паролем, состоящим из 3-х цифр. Выполните попытку подбора пароля с использованием программного обеспечения. В отчете отразить: контрольную сумму исходного файла, сжатого файла, выдаваемые сообщения, время подбора	ПК-3	У.6
8	Восстановите файл (.doc, .docx, .xls, .xlsx) , зараженный макровирусом (не используя антивирусную программу). Затем включите защиту от запуска макросов.	ПК-3	Н.5
9	Проверьте потенциальные места записей «троянских программ» в системном реестре ОС	ПК-3	Н.5
10	На основании предоставленного перечня информационных активов (ИА) предприятия распределите информационные активы на: составляющие коммерческую тайну, персональные данные и открытые активы.	ПК-3	У.6
11	Укажите в подготовленном перечне сведения, доступ к которым не может быть ограничен	ПК-3	Н.5
12	Охарактеризуйте структуру правовых актов, ориентированных на правовую защиту информации	ПК-3	У.6
13	Укажите как подразделяется информация ограниченного доступа в соответствии с ФЗ-149?	ПК-3	У.6
14	Выделите информацию конфиденциального характера	ПК-3	Н.5
15	Выделите информацию ограниченного доступа	ПК-3	Н.5
16	Выделите основные организационные мероприятия по защите информации	ПК-3	Н.5
17	Перечислите 6 видов информации конфиденциального характера	ПК-3	У.6
18	Создайте в Outlook Express систему правил по обработке входящих сообщений электронной почты	ПК-3	Н.5
19	Для отправления сообщения в Outlook Express , подписанного цифровой подписью и зашифрованного, получите цифровой идентификатор	ПК-3	Н.5
20	Настройте параметры локальной политики безопасности ОС	ПК-3	Н.5
21	Создайте учетную запись и локальную группу, измените принадлежность пользователя к локальной группе и заблокируйте учетную запись пользователя	ПК-3	Н.5
22	Загрузите редактор Шаблона безопасности, отредактируйте (модифицируйте настройку безопасности) шаблон безопасности и сохраните его с новым именем	ПК-3	Н.5

23	Создайте VPN-подключение и выполните его настройку	ПК-3	Н.5
24	Используя метод шифрования - "перестановка", зашифровать свои данные: фамилию, имя, отчество	ПК-3	У.6
25	Используя метод шифрования - "замена", зашифровать свои данные: фамилию, имя, отчество	ПК-3	У.6
26	Определите примерный перечень сведений, составляющих коммерческую (служебную) тайну предприятия	ПК-3	У.6
27	Укажите последовательность действий в системе КриптоАРМ при выполнении подписания документа	ПК-3	Н.5
28	Укажите последовательность действий в системе КриптоАРМ для выполнения открытия документа	ПК-3	Н.5
29	Разработать Политику безопасности объекта	ПК-3	Н.5
30	Разработать Концептуальную модель информационной безопасности объекта	ПК-3	Н.5

5.3.2.4. Перечень тем рефератов, контрольных, расчетно-графических работ

Не предусмотрены

5.3.2.5. Вопросы для контрольной (расчетно-графической) работы

Не предусмотрены

5.4. Система оценивания достижения компетенций

5.4.1. Оценка достижения компетенций в ходе промежуточной аттестации

ПК-3 Способен составлять прогнозы динамики основных экономических показателей деятельности хозяйствующих субъектов с учетом возможных экономических рисков и угроз экономической безопасности			
Индикаторы достижения компетенции ПК-3		Номера вопросов и задач	
Код	Содержание	вопросы к зачету с оценкой	задачи к зачету с оценкой
З.6	**Знать** основные виды угроз информационной безопасности организаций	1-30	
У.6	**Уметь** проводить исследования в целях определения потенциальных и реальных угроз информационной безопасности организации		1-5, 7,9,14-16
Н.5	**Иметь навыки** осуществления мероприятий, направленных на определение потенциальных и реальных угроз информационной безопасности организации		6, 8, 10-13, 17-18

5.4.2. Оценка достижения компетенций в ходе текущего контроля

ПК-3 Способен составлять прогнозы динамики основных экономических показателей деятельности хозяйствующих субъектов с учетом возможных экономических рисков и угроз экономической безопасности				
Индикаторы достижения компетенции ПК-3		Номера вопросов и задач		
Код	Содержание	вопросы тестов	вопросы устного опроса	задачи для проверки умений и навыков
З.6	**Знать** основные виды угроз информационной безопасности организаций	1, 3-7, 13-16, 18-65, 69-77, 79-97, 99-106, 108-139	1-7, 9-22, 25, 27-29, 31-34, 37-46, 49, 51-61, 63-67, 69-73, 75-79, 81-85, 87-98	
У.6	**Уметь** проводить исследования в целях определения потенциальных и реальных угроз информационной безопасности организации	2, 8-12, 17, 66-68, 78, 98, 107	8, 23-24, 26, 30, 35-36, 42, 47-48, 50, 62, 68, 74, 80, 86, 92	1-7, 10, 12-13, 17, 24-26
Н.5	**Иметь навыки** осуществления мероприятий, направленных на определение потенциальных и реальных угроз информационной безопасности организации			8, 9, 11, 14-16, 18-23, 27-30

6. Учебно-методическое обеспечение дисциплины

6.1. Рекомендуемая литература

Тип рекомендаций	Перечень и реквизиты литературы (автор, название, год и место издания)	Количество экз. в библиотеке
1	2	3
2.1. Учебные издания	Баранова Е. К. Информационная безопасность. История специальных методов криптографической деятельности [электронный ресурс]: Учебное пособие / Е. К. Баранова, А. В. Бабаш, Д. А. Ларин; Национальный исследовательский университет "Высшая школа экономики" - Москва: Издательский Центр РИОР, 2022 - 236 с. [ЭИ] [ЭБС Знаниум] URL: https://znanium.com/catalog/document?id=388319	-
	Болелов Э. А. Информационный мир XXI века. Криптография- основа информационной безопасности [электронный ресурс]: Учебно-методическая литература / Э. А. Болелов - Москва: Издательско-торговая корпорация "Дашков и К", 2020 - 126 с. [ЭИ] [ЭБС Знаниум] URL: https://znanium.com/catalog/document?id=353538	-
	Горюхина Е. Ю. Информационная безопасность [Электронный ресурс]: практикум для аудиторных занятий для студентов, обучающихся по специальности 38.05.01 "Экономическая безопасность" / Е. Ю. Горюхина, И. М. Семенова, Е. П. Суворова; Воронежский государственный аграрный университет - Воронеж: Воронежский государственный аграрный университет, 2015 [ПТ] URL: http://catalog.vsau.ru/elib/books/b107312.pdf	1
	Горюхина Е. Ю. Информационная безопасность: учебное пособие: для студентов, обучающихся по специальности 38.05.01 "Экономическая безопасность" / Е. Ю. Горюхина, Л. И. Литвинова, Н. В. Ткачева; Воронежский государственный аграрный университет - Воронеж: Воронежский государственный аграрный университет, 2015 - 221 с. [ЦИТ 13054] [ПТ] URL: http://catalog.vsau.ru/elib/books/b107623.pdf	40
	Ищейнов В. Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации [электронный ресурс]: Учебное пособие / В. Я. Ищейнов, М. В. Мецатунян; Политехнический колледж № 8 имени дважды Героя Советского Союза И.Ф. Павлова - Москва: ООО "Научно-издательский центр ИНФРА-М", 2022 - 256 с. [ЭИ] [ЭБС Знаниум] URL: https://znanium.com/catalog/document?id=395132	-
	Рычаго М. Е. Основы защиты информации [электронный ресурс]: Учебное пособие / М. Е. Рычаго, И. В. Ершова, Р. Н. Тихомиров - Владимир: ФГОУ ВПО "Владимирский юридический институт Федеральной службы исполнения наказаний", 2017 - 68 с. [ЭИ] [ЭБС Знаниум] URL: https://znanium.com/catalog/document?id=395218	-

Тип рекомендаций	Перечень и реквизиты литературы (автор, название, год и место издания)	Количество экз. в библиотеке
1	2	3
	Сулейманов М. Д. Цифровая экономика [Электронный ресурс]: учебник / М. Д. Сулейманов - Сочи: РосНОУ, 2020 - 356 с. [ЭИ] [ЭБС Лань] URL: https://e.lanbook.com/book/162182	-
2.2. Методические издания	Горюхина Е. Ю. Информационная безопасность [Электронный ресурс]: практикум: учебно-методическое пособие для аудиторной и самостоятельной работы студентов экономического факультета, обучающихся по специальности Экономическая безопасность / Е. Ю. Горюхина, И. М. Семенова, С. М. Кусмагамбетов; Воронежский государственный аграрный университет - Воронеж: Воронежский государственный аграрный университет, 2022 [ПТ] URL: http://catalog.vsau.ru/elib/books/b167450.pdf	1
2.3. Периодические издания	Информатика: ежеквартальный научный журнал / Учредитель и издатель: Объединенный институт проблем информатики НАН Беларуси - Минск: Объединенный институт проблем информатики НАН Беларуси, 2020 [ЭИ] URL: https://elibrary.ru/contents.asp?titleid=64817	1

6.2. Ресурсы сети Интернет

6.2.1. Электронные библиотечные системы

№	Название	Размещение
1	Лань	https://e.lanbook.com
2	ZNANIUM.COM	http://znanium.com/
3	Национальная электронная библиотека (НЭБ	https://rusneb.ru/
4	E-library	https://elibrary.ru/
5	Электронная библиотека ВГАУ	http://library.vsau.ru/

6.2.2. Профессиональные базы данных и информационные системы

№	Название	Адрес доступа
1	Единая межведомственная информационно-статистическая система	https://fedstat.ru/
2	База данных показателей муниципальных образований	http://www.gks.ru/free_doc/new_site/bd_munst/munst.htm
3	База данных ФАОСТАТ	http://www.fao.org/faostat/ru/
4	Портал открытых данных РФ	https://data.gov.ru/
5	Портал государственных услуг	https://www.gosuslugi.ru/
6	Единая информационная система в сфере закупок	http://zakupki.gov.ru
7	Электронный сервис "Прозрачный бизнес"	https://pb.nalog.ru
8	Справочная правовая система Консультант Плюс	http://www.consultant.ru/
9	Справочная правовая система Гарант	http://ivo.garant.ru
10	Федеральная государственная система территориального планирования	https://fgistp.economy.gov.ru/
11	Аграрная российская информационная система.	http://www.aris.ru/
12	Информационная система по сельскохозяйственным наукам и технологиям	http://agris.fao.org/

6.2.3. Сайты и информационные порталы

№	Название	Размещение
1.	Информационно-аналитический портал в сфере информационной безопасности	https://www.securitylab.ru/
2	Аналитический центр информационной безопасности	https://www.infowatch.ru/analytics
3.	Журнал «Мир безопасности»	http://id-mb.ru/zhurnal/
4.	Журнал «Information Security/Информационная безопасность»	http://www.itsec.ru/information-security

7. Материально-техническое и программное обеспечение дисциплины

7.1. Помещения для ведения образовательного процесса и оборудование

Наименование помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом, в том числе помещения для самостоятельной работы, с указанием перечня основного оборудования, учебно-наглядных пособий и используемого программного обеспечения	Адрес (местоположение) помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом (в случае реализации образовательной программы в сетевой форме дополнительно указывается наименование организации, с которой заключен договор)
Учебная аудитория для проведения учебных занятий: комплект учебной мебели, демонстрационное оборудование и учебно-наглядные пособия, презентационное оборудование, используемое программное обеспечение: MS Windows; Office MS Windows / Open Office; Adobe Reader / DjVu Reader; Яндекс Браузер / Mozilla Firefox / Internet Explorer; DrWeb ES; 7-Zip; Media Player Classic	394087, Воронежская область, г. Воронеж, ул. Мичурина, 1
Учебная аудитория для проведения учебных занятий: комплект учебной мебели, демонстрационное оборудование и учебно-наглядные пособия, компьютеры в аудитории с выходом в локальную сеть и Интернет; доступ к справочно-правовым системам «Гарант» и «Консультант Плюс»; электронные учебно-методические материалы; видеопроекционное оборудование для презентаций; используемое программное обеспечение: MS Windows; Office MS Windows / Open Office; Adobe Reader / DjVu Reader; Яндекс Браузер / Mozilla Firefox / Internet Explorer; DrWeb ES; 7-Zip; Media Player Classic	394087, Воронежская область, г. Воронеж, ул. Мичурина, 1
Учебная аудитория для проведения учебных занятий: для текущего контроля и промежуточной аттестации: комплект учебной мебели, демонстрационное оборудование и учебно-наглядные пособия, компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду, используемое программное обеспечение: MS Windows; Office MS Windows / Open Office;	394087, Воронежская область, г. Воронеж, ул. Мичурина, 1

Adobe Reader / DjVu Reader; Яндекс Браузер / Mozilla Firefox / Internet Explorer; DrWeb ES; 7-Zip; Media Player Classic, AST Test	
Учебная аудитория для проведения учебных занятий: для групповых и индивидуальных консультаций: комплект учебной мебели, компьютеры, принтеры, сканер, используемое программное обеспечение: MS Windows; Office MS Windows / Open Office; Adobe Reader / DjVu Reader; Яндекс Браузер / Mozilla Firefox / Internet Explorer; DrWeb ES; 7-Zip; Media Player Classic	394087, Воронежская область, г. Воронеж, ул. Мичурина, 1
Помещение для самостоятельной работы: комплект учебной мебели, компьютерная техника с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду, используемое программное обеспечение: MS Windows; Office MS Windows / Open Office; Adobe Reader / DjVu Reader; Яндекс Браузер / Mozilla Firefox / Internet Explorer; DrWeb ES; 7-Zip; Media Player Classic	394087, Воронежская область, г. Воронеж, ул. Мичурина, 1, ауд. 113, 115, 116, 119 120, 122, 123а, 126, 219, 220, 224, 241, 273 (с 16.00 до 20.00)
Помещение для самостоятельной работы: комплект учебной мебели, компьютерная техника с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду, используемое программное обеспечение: MS Windows; Office MS Windows / Open Office; Adobe Reader / DjVu Reader; Яндекс Браузер / Mozilla Firefox / Internet Explorer; DrWeb ES; 7-Zip; Media Player Classic	394087, Воронежская область, г. Воронеж, ул. Мичурина, 1, ауд. 232 а

7.2. Программное обеспечение

7.2.1. Программное обеспечение общего назначения

№	Название	Размещение
1	Операционные системы MS Windows / Linux	ПК в локальной сети ВГАУ
2	Пакеты офисных приложений Office MS Windows / OpenOffice	ПК в локальной сети ВГАУ
3	Программы для просмотра файлов AdobeReader / DjVuReader	ПК в локальной сети ВГАУ
4	Браузеры Яндекс Браузер / Mozilla Firefox / Internet Explorer	ПК в локальной сети ВГАУ
5	Антивирусная программа DrWeb ES	ПК в локальной сети ВГАУ
6	Программа-архиватор 7-Zip	ПК в локальной сети ВГАУ
7	Мультимедиа проигрыватель MediaPlayerClassic	ПК в локальной сети ВГАУ
8	Платформа онлайн-обучения eLearning server	ПК в локальной сети ВГАУ
9	Система компьютерного тестирования AST Test	ПК в локальной сети ВГАУ

7.2.2. Специализированное программное обеспечение

Не требуется

8. Междисциплинарные связи

Дисциплина, с которой необходимо согласование	Кафедра, на которой преподается дисциплина	Подпись заведующего кафедрой
Б1.О.13 Экономическая безопасность	Экономики АПК	
Б1.В.01 Безопасность электронного документооборота	Информационного обеспечения и моделирования агроэкономических систем	
Б1.В.10 Современные платежные системы и их безопасность	Информационного обеспечения и моделирования агроэкономических систем	

Приложение 1

Лист изменений рабочей программы

Номер изменения	Номер протокола заседания кафедры и дата	Страницы с изменениями	Перечень откорректированных пунктов	Подпись заведующего кафедрой

Приложение 2

Лист периодических проверок рабочей программы и информация о внесенных изменениях

Должностное лицо, проводившего проверку: Ф.И.О., должность, подпись	Дата	Потребность в корректировке	Перечень пунктов, страниц, разделов, требующих изменений
Зав. кафедрой Подколзин Р.В	Протокол № 8 от 26.04.2024 г.	Рабочая программа актуализирована на 2024-2025 учебный год	