Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«Самарский государственный экономический университет»

Институт Институт экономики предприятий

Кафедра Прикладной информатики

УТВЕРЖДЕНО
Ученым советом Университета
(протокол № 10 от 22 мая 2025 г.)

РАБОЧАЯ ПРОГРАММА

Наименование дисциплины Б1.В.15 Компьютерная экспертиза

Основная профессиональная образовательная программа 09.03.03 Прикладная информатика программа Прикладная информатика и защита информации

Квалификация (степень) выпускника Бакалавр

Самара 2025

Содержание (рабочая программа)

Стр.

Целью изучения дисциплины является формирование результатов обучения, обеспечивающих достижение планируемых результатов освоения образовательной программы.

1. Место дисциплины в структуре ОП

Дисциплина Компьютерная экспертиза входит в часть, формируемая участниками образовательных отношений блока Б1.Дисциплины (модули)

Предшествующие дисциплины по связям компетенций: Хранение, обработка и анализ данных, Вычислительные системы, сети и телекоммуникации, Основы алгоритмизации и программирования, Основы проектной деятельности, Современные технологии и языки программирования, Теория информационной безопасности и методология защиты информации, Системы искусственного интеллекта, Облачные технологии и услуги, Технологии защищенного документооборота

Последующие дисциплины по связям компетенций: Разработка профессиональных приложений, Проектный практикум, Проектирование информационных систем, Управление информационной безопасностью, Специализированные ИТ в правоохранительной деятельности, Управление информационными проектами реализации комплексной безопасности, Цифровая культура в профессиональной деятельности, Интеллектуальные информационные системы, Современные цифровые технологии управления предприятием

2. Планируемые результаты обучения по дисциплине, обеспечивающие достижение планируемых результатов обучения по программе

Изучение дисциплины Компьютерная экспертиза в образовательной программе направлено на формирование у обучающихся следующих компетенций:

Профессиональные компетенции (ПК):

ПК-1 - Способен к обнаружению и идентификации инцидентов в процессе эксплуатации автоматизированной системы

Планируемые результаты обучения по программе	**Планируемые результаты обучения по дисциплине**		
ПК-1	ПК-1.1: Знать:	ПК-1.2: Уметь:	ПК-1.3: Владеть (иметь навыки):
	особенности инцидентов в процессе эксплуатации автоматизированной системы	обнаруживать и идентифицировать инциденты в процессе эксплуатации автоматизированной системы	навыками обнаружения и идентификации инцидентов в процессе эксплуатации автоматизированной системы

3. Объем и виды учебной работы

Учебным планом предусматриваются следующие виды учебной работы по дисциплине:

Очная форма обучения

Виды учебной работы	Всего час/ з.е.
	Сем 6
Контактная работа, в том числе:	36.15/1
Занятия лекционного типа	18/0.5
Занятия семинарского типа	18/0.5
Индивидуальная контактная работа (ИКР)	0.15/0
Самостоятельная работа:	17.85/0.5
Промежуточная аттестация	18/0.5
Вид промежуточной аттестации: Зачет	Зач
Общая трудоемкость (объем части образовательной	

программы): Часы Зачетные единицы	72 2

очно-заочная форма

Виды учебной работы	Всего час/ з.е.
	Сем 7
Контактная работа, в том числе:	4.15/0.12
Занятия лекционного типа	2/0.06
Занятия семинарского типа	2/0.06
Индивидуальная контактная работа (ИКР)	0.15/0
Самостоятельная работа:	49.85/1.38
Промежуточная аттестация	18/0.5
Вид промежуточной аттестации: Зачет	Зач
Общая трудоемкость (объем части образовательной программы): Часы Зачетные единицы	72 2

4. Содержание дисциплины

4.1. Разделы, темы дисциплины и виды занятий:

Тематический план дисциплины Компьютерная экспертиза представлен в таблице.

Разделы, темы дисциплины и виды занятий
Очная форма обучения

№ п/п	Наименование темы (раздела) дисциплины	Контактная работа				Самостоятельная работа	Планируемые результаты обучения в соотношении с результатами обучения по образовательной программе
		Лекции	Занятия семинарского типа	ИКР	ГКР		
			Практич. занятия				
1.	Общие положения. Предмет и задачи теории компьютерной экспертизы	8	8	0.1		10	ПК-1.1, ПК-1.2, ПК-1.3
2.	Нормативно-правовые и научные основы проведения компьютерно-технических экспертиз. Понятия компьютерно-технической экспертиз. Понятие надежной безопасности. Методы проведения компьютерно-технической экспертизы.	10	10	0.05		7.85	ПК-1.1, ПК-1.2, ПК-1.3
	Контроль	18					
	Итого	**18**	**18**	**0.15**		**17.85**	

очно-заочная форма

№ п/п	Наименование темы (раздела) дисциплины	Контактная работа				Самостоятельная работа	Планируемые результаты обучения в соотношении с результатами
		Лекции	Занятия семинарского типа	ИКР	ГКР		
			Практич. занятия				

							обучения по образовательной программе
1.	Общие положения. Предмет и задачи теории компьютерной экспертизы	1	1	0,075		24	ПК-1.1, ПК-1.2, ПК -1.3
2.	Нормативно-правовые и научные основы проведения компьютерно-технических экспертиз. Понятия компьютерно-технической экспертиз. Понятие надежной безопасности. Методы проведения компьютерно-технической экспертизы.	1	1	0,075		25,85	ПК-1.1, ПК-1.2, ПК -1.3
	Контроль	18					
	Итого	**2**	**2**	0.15		**49.85**	

4.2 Содержание разделов и тем

4.2.1 Контактная работа

Тематика занятий лекционного типа

№п/п	**Наименование темы (раздела) дисциплины**	**Вид занятия лекционного типа***	**Тематика занятия лекционного типа**
1.	Общие положения. Предмет и задачи теории компьютерной экспертизы	лекция	Анализ нормативно-правовых и научных основ проведения компьютернотехнических экспертиз
		лекция	Специальная методология криминалистики и судебной экспертизы как проблема.
		лекция	Исследование компьютерно-технических средств
		лекция	Уголовно-правовая характеристика и особенности юридической квалификации преступлений, сопряженных с применением компьютерных средств
2.	Нормативно-правовые и научные основы проведения компьютерно-технических экспертиз. Понятия компьютерно-технической экспертиз. Понятие надежной безопасности. Методы проведения компьютерно-технической экспертизы.	лекция	Компьютерно-Технические Экспертизы
		лекция	Анализ методик производства КТЭ
		лекция	Методика Проведения Компьютерно-Технической Экспертизы
		лекция	Оценка эффективности разработанной методики производства экспертизы
		лекция	Формы использования в уголовном и гражданском судопроизводстве специальных познаний в сфере современных информационных технологий.

*лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации педагогическими работниками организации и (или) лицами, привлекаемыми организацией к реализации образовательных программ на иных условиях, обучающимся

Тематика занятий семинарского типа

№п/п	Наименование темы (раздела) дисциплины	Вид занятия семинарского типа**	Тематика занятия семинарского типа
1.	Общие положения. Предмет и задачи теории компьютерной экспертизы	практическое занятие	Анализ нормативно-правовых и научных основ проведения компьютернотехнических экспертиз
		практическое занятие	Специальная методология криминалистики и судебной экспертизы как проблема.
		практическое занятие	Исследование компьютерно-технических средств
		практическое занятие	Уголовно-правовая характеристика и особенности юридической квалификации преступлений, сопряженных с применением компьютерных средств
2.	Нормативно-правовые и научные основы проведения компьютерно-технических экспертиз. Понятия компьютерно-технической экспертиз. Понятие надежной безопасности. Методы проведения компьютерно-технической экспертизы.	практическое занятие	Компьютерно-Технические Экспертизы
		практическое занятие	Анализ методик производства КТЭ
		практическое занятие	Методика Проведения Компьютерно-Технической Экспертизы
		практическое занятие	Оценка эффективности разработанной методики производства экспертизы
		практическое занятие	Формы использования в уголовном и гражданском судопроизводстве специальных познаний в сфере современных информационных технологий.

** семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия

Иная контактная работа

При проведении учебных занятий СГЭУ обеспечивает развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств (включая при необходимости проведение интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализ ситуаций и имитационных моделей, преподавание дисциплин (модулей) в форме курсов, составленных на основе результатов научных исследований, проводимых организацией, в том числе с учетом региональных особенностей профессиональной деятельности выпускников и потребностей работодателей).

Формы и методы проведения иной контактной работы приведены в Методических указаниях по основной профессиональной образовательной программе.

4.2.2 Самостоятельная работа

№п/п	Наименование темы (раздела) дисциплины	Вид самостоятельной работы ***
1.	Общие положения. Предмет и задачи теории компьютерной экспертизы	- подготовка доклада - подготовка электронной презентации - тестирование
2.	Нормативно-правовые и научные основы проведения компьютерно-технических экспертиз. Понятия компьютерно-технической экспертиз. Понятие надежной безопасности. Методы проведения компьютерно-технической экспертизы.	- подготовка доклада - подготовка электронной презентации - тестирование

*** самостоятельная работа в семестре, написание курсовых работ, докладов, выполнение контрольных работ

5. Материально-техническое и учебно-методическое обеспечение дисциплины

5.1 Литература:

Основная литература

1. Манучарян, А. К. Комплексные аспекты компьютерно-технической экспертизы : учебное пособие / А. К. Манучарян. — Москва : Московский государственный технический университет имени Н.Э. Баумана, 2020. — 28 с. — ISBN 978-5-7038-5376-4. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/115332.html

Дополнительная литература

1. Расследование преступлений в сфере компьютерной информации и электронных средств платежа : учебное пособие для вузов / С. В. Зуев [и др.] ; ответственные редакторы С. В. Зуев, В. Б. Вехов. — Москва : Издательство Юрайт, 2024. — 243 с. — (Высшее образование). — ISBN 978-5-534-13898-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/544035

2. Саркисян, А. А. Цифровизация судебно-экспертной деятельности : учебное пособие для вузов / А. А. Саркисян. — Москва : Издательство Юрайт, 2025. — 138 с. — (Высшее образование). — ISBN 978-5-534-20447-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/558168

3. Цифровая криминалистика : учебник для вузов / В. Б. Вехов [и др.] ; под редакцией В. Б. Вехова, С. В. Зуева. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 490 с. — (Высшее образование). — ISBN 978-5-534-17464-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/568013

Литература для самостоятельного изучения

1.

5.2. Перечень лицензионного программного обеспечения

1. Astra Linux Special Edition «Смоленск», «Орел»; РедОС ; ОС "Альт Рабочая станция" 10; ОС "Альт Образование" 10
2. МойОфис Стандартный 2, МойОфис Образование, Р7-Офис Профессиональный, МойОфис Стандартный 3, МойОфис Профессиональный 3

5.3 Современные профессиональные базы данных, к которым обеспечивается доступ обучающихся

1. Профессиональная база данных «Информационные системы Министерства экономического развития Российской Федерации в сети Интернет» (Портал «Официальная Россия» - http://www.gov.ru/)
2. Государственная система правовой информации «Официальный интернет-портал правовой информации» (http://pravo.gov.ru/)
3. Профессиональная база данных «Финансово-экономические показатели Российской Федерации» (Официальный сайт Министерства финансов РФ - https://www.minfin.ru/ru/)
4. Профессиональная база данных «Официальная статистика» (Официальный сайт Федеральной службы государственной статистики - http://www.gks.ru/

5.4. Информационно-справочные системы, к которым обеспечивается доступ обучающихся

1. Справочно-правовая система «Консультант Плюс»
2. Справочно-правовая система «ГАРАНТ-Максимум»

5.5. Специальные помещения

Учебные аудитории для проведения занятий лекционного типа	Комплекты ученической мебели Мультимедийный проектор Доска

	Экран
Учебные аудитории для проведения практических занятий (занятий семинарского типа)	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГЭУ
Учебные аудитории для групповых и индивидуальных консультаций	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГЭУ
Учебные аудитории для текущего контроля и промежуточной аттестации	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГЭУ
Помещения для самостоятельной работы	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГЭУ
Помещения для хранения и профилактического обслуживания оборудования	Комплекты специализированной мебели для хранения оборудования

5.6 Лаборатории и лабораторное оборудование

Лаборатория информационных технологий в профессиональной деятельности	Комплекты ученической мебели Мульмедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГЭУ Лабораторное оборудование

6. Фонд оценочных средств по дисциплине Компьютерная экспертиза:

6.1. Контрольные мероприятия по дисциплине

Вид контроля	**Форма контроля**	**Отметить нужное знаком « + »**
Текущий контроль	Оценка докладов	+
	Тестирование	+
	Практические задачи	+
Промежуточный контроль	Зачет	+

Порядок проведения мероприятий текущего и промежуточного контроля определяется Методическими указаниями по основной профессиональной образовательной программе высшего образования; Положением о балльно-рейтинговой системе оценки успеваемости обучающихся по основным образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам

магистратуры в федеральном государственном автономном образовательном учреждении высшего образования «Самарский государственный экономический университет».

6.2. Планируемые результаты обучения по дисциплине, обеспечивающие достижение планируемых результатов обучения по программе

Профессиональные компетенции (ПК):

ПК-1 - Способен к обнаружению и идентификации инцидентов в процессе эксплуатации автоматизированной системы

Планируемые результаты обучения по программе	**Планируемые результаты обучения по дисциплине**		
	ПК-1.1: Знать:	ПК-1.2: Уметь:	ПК-1.3: Владеть (иметь навыки):
	особенности инцидентов в процессе эксплуатации автоматизированной системы	обнаруживать и идентифицировать инциденты в процессе эксплуатации автоматизированной системы	навыками обнаружения и идентификации инцидентов в процессе эксплуатации автоматизированной системы
Пороговый	Особенности при сбоях функционирования вычислительной сети Локализовать отказы вычислительной сети Навыками обнаружения отказов вычислительной сети	Особенности при сбоях функционирования вычислительной сети Локализовать отказы вычислительной сети Навыками обнаружения отказов вычислительной сети	Особенности при сбоях функционирования вычислительной сети Локализовать отказы вычислительной сети Навыками обнаружения отказов вычислительной сети
Стандартный (в дополнение к пороговому)	Особенности при отказах функционирования Локализовать и идентифицировать Навыками обнаружения и идентификации отказов пороговому) вычислительной сети отказы вычислительной сети вычислительной сети	Особенности при отказах функционирования Локализовать и идентифицировать Навыками обнаружения и идентификации отказов пороговому) вычислительной сети отказы вычислительной сети вычислительной сети	Особенности при отказах функционирования Локализовать и идентифицировать Навыками обнаружения и идентификации отказов пороговому) вычислительной сети отказы вычислительной сети вычислительной сети
Повышенный (в дополнение к пороговому, стандартному)	Особенности при целенаправленном воздействии на функционирование вычислительной сети Локализовать и идентифицировать отказы вычислительной сети при целенаправленном воздействии на неё	Особенности при целенаправленном воздействии на функционирование вычислительной сети Локализовать и идентифицировать отказы вычислительной сети при целенаправленном	Особенности при целенаправленном воздействии на функционирование вычислительной сети Локализовать и идентифицировать отказы вычислительной сети при целенаправленном воздействии на неё

	Навыками обнаружения и идентификации отказов вычислительной сети при целенаправленном воздействии на неё	воздействии на неё Навыками обнаружения и идентификации отказов вычислительной сети при целенаправленном воздействии на неё	Навыками обнаружения и идентификации отказов вычислительной сети при целенаправленном воздействии на неё

6.3. Паспорт оценочных материалов

№ п/п	Наименование темы (раздела) дисциплины	Контролируемые планируемые результаты обучения в соотношении с результатами обучения по программе	Вид контроля/используемые оценочные средства	
			Текущий	Промежуточный
1.	Общие положения. Предмет и задачи теории компьютерной экспертизы	ПК-1.1, ПК-1.2, ПК-1.3	Оценка докладов Практические работы Тестирование	Зачет
2.	Нормативно-правовые и научные основы проведения компьютерно-технических экспертиз. Понятия компьютерно-технической экспертиз. Понятие надежной безопасности. Методы проведения компьютерно-технической экспертизы.	ПК-1.1, ПК-1.2, ПК-1.3	Оценка докладов Практические работы Тестирование	Зачет

6.4.Оценочные материалы для текущего контроля

Примерная тематика докладов

Раздел дисциплины	Темы
Общие положения. Предмет и задачи теории компьютерной экспертизы	1. Информация - фактор существования и развития общества. Основные формы проявления информации, её свойства как объекта безопасности. 2. Понятие безопасности и её составляющие. Безопасность информации. 3. Обеспечение информационной безопасности: содержание и структура понятия. 4. Национальные интересы в информационной сфере. 5. Источники и содержание угроз в информационной сфере. 6. Соотношение понятий «информационная безопасность» и «национальная безопасность» 7. Понятие национальной безопасности. Интересы и угрозы в области национальной безопасности. 8. Влияние процессов информатизации общества на составляющие национальной безопасности и их содержание.

	9. Система обеспечения информационной безопасности. 10.Обеспечение информационной безопасности Российской Федерации. 11.Понятие информационной войны. Проблемы информационной войны. 12. Информационное оружие и его классификация. 13. Цели информационной войны, её составные части и средства её ведения. Объекты воздействия в информационной войне. 14. Уровни ведения информационной войны. Информационные операции. Психологические операции. 15. Уровни ведения информационной войны. Оперативная маскировка. Радиоэлектронная борьба. Воздействие на сети.
Нормативно-правовые и научные основы проведения компьютерно-технических экспертиз. Понятия компьютерно-технической экспертиз. Понятие надежной безопасности. Методы проведения компьютерно-технической экспертизы.	16.Основные положения государственной информационной политики Российской Федерации. 17.Первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности. 18.Виды защищаемой информации в сфере государственного и муниципального управления. 19.Обеспечение информационной безопасности организации. 20.Характеристика эффективных стандартов по безопасности. 21.Требования к полноте эффективных стандартов по безопасности. 22.Риск работы на персональном компьютере. Планирование безопасной работы на персональном компьютере. 23. Информация - фактор существования и развития общества. 24.Обеспечение информационной безопасности: содержание и структура понятия. 25.Система обеспечения информационной безопасности. Обеспечение информационной безопасности организации. 26.Обеспечение информационной безопасности Российской Федерации. 27.Международная нормативная база обеспечения безопасности. Федеральная нормативная база обеспечения безопасности 28.Организационные структуры государственной системы обеспечения информационной безопасности федеральных органов исполнительной власти. 29. Административный уровень обеспечения информационной безопасности. 30.Организационные структуры системы обеспечения информационной безопасности предприятия (организации). 31.Корпоративная нормативная база по защите информации. 32.Основные организационные мероприятия по обеспечению информационной безопасности организации (предприятия). 33.Основные организационные мероприятия по обеспечению информационной безопасности организации (предприятия). 34.Нормативно-методические документы по обеспечению безопасности информации.

Задания для тестирования по дисциплине для оценки сформированности компетенций (min 20, max 50 + ссылку на ЭИОС с тестами)

https://lms2.sseu.ru/course/index.php?categoryid=1918

К правовым методам, обеспечивающим информационную безопасность, относятся:

- Разработка аппаратных средств обеспечения правовых данных

- Разработка и установка во всех компьютерных правовых сетях журналов учета действий

+ Разработка и конкретизация правовых нормативных актов обеспечения безопасности

Основными источниками угроз информационной безопасности являются все указанное в списке:

- Хищение жестких дисков, подключение к сети, инсайдерство

+ Перехват данных, хищение данных, изменение архитектуры системы

- Хищение данных, подкуп системных администраторов, нарушение регламента работы

Виды информационной безопасности:

+ Персональная, корпоративная, государственная

- Клиентская, серверная, сетевая

- Локальная, глобальная, смешанная

Цели информационной безопасности – своевременное обнаружение, предупреждение:

+ несанкционированного доступа, воздействия в сети

- инсайдерства в организации

- чрезвычайных ситуаций

Основные объекты информационной безопасности:

+ Компьютерные сети, базы данных

- Информационные системы, психологическое состояние пользователей

- Бизнес-ориентированные, коммерческие системы

Основными рисками информационной безопасности являются:

- Искажение, уменьшение объема, перекодировка информации

- Техническое вмешательство, выведение из строя оборудования сети

+ Потеря, искажение, утечка информации

К основным принципам обеспечения информационной безопасности относится:

+ Экономической эффективности системы безопасности

- Многоплатформенной реализации системы

- Усиления защищенности всех звеньев системы

Основными субъектами информационной безопасности являются:

- руководители, менеджеры, администраторы компаний

+ органы права, государства, бизнеса

- сетевые базы данных, фаерволлы

К основным функциям системы безопасности можно отнести все перечисленное:

+ Установление регламента, аудит системы, выявление рисков

- Установка новых офисных приложений, смена хостинг-компании

- Внедрение аутентификации, проверки контактных данных пользователей

тест

Принципом информационной безопасности является принцип недопущения:

+ Неоправданных ограничений при работе в сети (системе)

- Рисков безопасности сети, системы

- Презумпции секретности

Принципом политики информационной безопасности является принцип:

+ Невозможности миновать защитные средства сети (системы)

- Усиления основного звена сети, системы

- Полного блокирования доступа при риск-ситуациях

Принципом политики информационной безопасности является принцип:

+ Усиления защищенности самого незащищенного звена сети (системы)

- Перехода в безопасное состояние работы сети, системы

- Полного доступа пользователей ко всем ресурсам сети, системы

Принципом политики информационной безопасности является принцип:

+ Разделения доступа (обязанностей, привилегий) клиентам сети (системы)

- Одноуровневой защиты сети, системы

- Совместимых, однотипных программно-технических средств сети, системы

К основным типам средств воздействия на компьютерную сеть относится:

- Компьютерный сбой

+ Логические закладки («мины»)

- Аварийное отключение питания

Когда получен спам по e-mail с приложенным файлом, следует:

- Прочитать приложение, если оно не содержит ничего ценного – удалить

- Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама

+ Удалить письмо с приложением, не раскрывая (не читая) его

Принцип Кирхгофа:

- Секретность ключа определена секретностью открытого сообщения

- Секретность информации определена скоростью передачи данных

+ Секретность закрытого сообщения определяется секретностью ключа

ЭЦП – это:

- Электронно-цифровой преобразователь

+ Электронно-цифровая подпись

- Электронно-цифровой процессор

Наиболее распространены угрозы информационной безопасности корпоративной системы:

- Покупка нелицензионного ПО

+ Ошибки эксплуатации и неумышленного изменения режима работы системы

- Сознательного внедрения сетевых вирусов

Наиболее распространены угрозы информационной безопасности сети:

- Распределенный доступ клиент, отказ оборудования

- Моральный износ сети, инсайдерство

+ Сбой (отказ) оборудования, нелегальное копирование данных

Наиболее распространены средства воздействия на сеть офиса:

- Слабый трафик, информационный обман, вирусы в интернет

+ Вирусы в сети, логические мины (закладки), информационный перехват

- Компьютерные сбои, изменение администрирования, топологии

6.5. Оценочные материалы для промежуточной аттестации

Фонд вопросов для проведения промежуточного контроля в форме зачета

Раздел дисциплины	Вопросы
Общие положения. Предмет и задачи теории защиты информации	1. Какова общая характеристика представленного программного обеспечения, из каких компонент (программных средств) оно состоит? 2. Какую классификацию имеют конкретные программные средства (системные или прикладные) представленного программного обеспечения?

	3. Каковы наименование, тип, версия, вид представления (явный, скрытый, удаленный) программного средства? 4. Каковы реквизиты разработчика и владельца данного программного средства? 5. Каков состав соответствующих файлов программного обеспечения, каковы их параметры (объемы, даты создания, атрибуты)? 6. Какое общее функциональное предназначение имеет программное средство? 7. Имеются ли на носителях информации программные средства для реализации определенной функциональной задачи? 8. Какие требования предъявляет данное программное средство к аппаратным средствам компьютерной системы? 9. Какова совместимость конкретного программного средства с программным и аппаратным обеспечением компьютерной системы? 10. Используется ли данное программное средство для решения определенной функциональной задачи? 11. Каковы фактическое состояние программного средства, его работоспособность по реализации отдельных (конкретных) функций? 12. Каким образом организованы ввод и вывод данных в представленном программном средстве? 13. Имеются ли в программном средстве отклонения от нормальных параметров типовых программных продуктов (например, свойства инфицирования, недокументированных функций)?
Классификация угроз безопасности и уровней защиты. Интерпретация угрозы атаки. Понятие надежной безопасности. Методы и абстрактные модели защиты информации.	14. Имеет ли программное средство защитные возможности (программные, аппаратно-программные) от несанкционированного доступа и копирования? 15. Каким образом организованы защитные возможности программного средства? 16. Каков общий алгоритм данного программного средства? 17. Какие программные инструментальные средства (языки программирования, компиляторы, стандартные библиотеки) использовались при разработке данного программного средства? 18. Имеются ли на носителях информации тексты (коды) с первоначальным состоянием программы? 19. Подвергался ли алгоритм программного средства модификации по сравнению с исходным состоянием? В чем это нашло отражение? 20. Какой вид имело программное средство до его последней модификации? 21. Использованы ли в алгоритме программы и ее тексте какиелибо специфические (нестандартные) приемы алгоритмизации и программирования? 22. С какой целью было произведено изменение каких-либо функций в программном средстве? 23. Направлены ли внесенные изменения в программное средство на преодоление его защиты? 24. Достигается ли решение определенных задач после внесения изменений в программное средство? 25. Каким способом были произведены изменения в программе (преднамеренно, воздействием вредоносной программы, ошибками программной среды, аппаратным сбоем и др.)? 26. Какова хронология внесения изменений в программном средстве? 27. Какова хронология использования программного средства (начиная с ее инсталляции)?

6.6. Шкалы и критерии оценивания по формам текущего контроля и промежуточной аттестации

Шкала и критерии оценивания

Оценка	Критерии оценивания для мероприятий контроля с применением 2-х балльной системы
«зачтено»	ПК-1
«не зачтено»	Результаты обучения не сформированы на пороговом уровне