МИНОБРНАУКИ РОССИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«Кузбасский государственный технический университет имени Т.Ф. Горбачева»

Филиал КузГТУ в г. Новокузнецке

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 65A182AF55E85519218FE36C1C7FB48A
Владелец: Евсина Татьяна Алексеевна
Действителен: с 16.11.2022 до 09.02.2024

УТВЕРЖДАЮ
Директор филиала КузГТУ
_____ Т.А. Евсина
«29» мая 2023 г.

Фонд оценочных средств дисциплины
Техническая защита информации

Специальность
«10.02.05 Обеспечение информационной безопасности автоматизированных систем»

Присваиваемая квалификация
«Техник по защите информации»

Форма обучения
очная

Год набора 2022

Срок обучения на базе
среднего общего образования – 2 года 10 месяцев

Новокузнецк 2023 г.

1. Фонд оценочных средств для проведения текущего контроля, промежуточной аттестации обучающихся по дисциплине

1.1 Паспорт фонда оценочных средств

Планируемые результаты обучения по дисциплине.

Дисциплина направлена на формирование следующих компетенций выпускника:

Наименование разделов дисциплины	Содержание (темы) раздела	Код компетенции	Знания, умения, практический опыт, необходимые для формирования соответствующей компетенции	Форма текущего контроля знаний, умений, практического опыта, необходимых для формирования соответствующей компетенции
Раздел 1. Концепция инженерно-технической защиты информации	Тема 1.1. Предмет и задачи технической защиты информации Тема 1.2. Общие положения защиты информации техническими средствами	ОК 01	**Знать**: актуальный профессиональный и социальный контекст, в котором приходится работать и жить; **Уметь:** распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части;	опрос обучающихся по контрольным вопросам, защита отчетов по практическим заданиям, тестирование
		ОК 02	**Знать:** номенклатуру информационных источников применяемых в профессиональной деятельности; **Уметь:** определять задачи поиска информации;	
		ОК 03	**Знать:** содержание актуальной нормативно-правовой документации; современную научную и профессиональную терминологию; **Уметь:** определять актуальность нормативно-правовой документации в профессиональной деятельности;	
		ОК 09	**Знать:** современные средства и устройства информатизации; **Уметь: п**рименять средства информационных технологий для решения профессиональных задач;	
		ОК 10	**Знать:** правила построения простых и сложных предложений на профессиональные темы; **Уметь:** понимать общий смысл четко произнесенных	

			высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы;	
Раздел 2. Теоретические основы инженерно-технической защиты информации	Тема 2.1. Информация как предмет защиты Тема 2.2. Технические каналы утечки информации Тема 2.3. Методы и средства технической разведки	ОК 01	**Знать:** основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; **Уметь:** определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы;	опрос обучающихся по контрольным вопросам, защита отчетов по практическим заданиям, тестирование
		ОК 02	**Знать:** приемы структурирования информации; **Уметь:** определять необходимые источники информации;	
		ОК 03	**Знать:** возможные траектории профессионального развития и самообразования; **Уметь:** выстраивать траектории профессионального и личностного развития;	
		ОК 09	**Знать:** порядок их применения и программное обеспечение в профессиональной деятельности; **Уметь:** использовать современное программное обеспечение;	
		ОК 10	**Знать:** основные общеупотребительные глаголы (бытовая и профессиональная лексика); **Уметь:** участвовать в диалогах на знакомые общие и профессиональные темы;	
Раздел 3. Физические основы технической защиты информации	Тема 3.1. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок	ОК 01	**Знать:** алгоритмы выполнения работ в профессиональной и смежных областях; **Уметь:** составить план действия; определить необходимые ресурсы;	опрос обучающихся по контрольным вопросам, защита отчетов по практическим заданиям, тестирование
		ОК 02	**Знать:** формат оформления результатов поиска информации; **Уметь:** планировать процесс поиска; структурировать получаемую информацию;	

		ОК 09	**Знать:** современные средства и устройства информатизации; **Уметь:** применять средства информационных технологий для решения профессиональных задач;	
		ОК 10	**Знать:** лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; **Уметь:** строить простые высказывания о себе и о своей профессиональной деятельности;	
		ПК 3.3	**Знать:** номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации; **Уметь:** применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных; **Иметь практический опыт:** проведения измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации;	
		ПК 3.4	**Знать:** номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам; **Уметь:** применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных; **Иметь практический опыт:** проведения измерений параметров фоновых шумов, а также физических полей, создаваемых техническими	

			средствами защиты информации;	
Раздел 4. Системы защиты от утечки информации	Тема 4.1. Системы защиты от утечки информации по акустическому каналу Тема 4.2. Системы защиты от утечки информации по проводному каналу Тема 4.3. Системы защиты от утечки информации по вибрационному каналу Тема 4.4. Системы защиты от утечки информации по электромагнитному каналу Тема 4.5. Системы защиты от утечки информации по телефонному каналу Тема 4.6. Системы защиты от утечки информации по электросетевому каналу Тема 4.7. Системы защиты от утечки информации по оптическому каналу	ОК 01	**Знать**: методы работы в профессиональной и смежных сферах; структуру плана для решения задач; **Уметь:** владеть актуальными методами работы в профессиональной и смежных сферах;	опрос обучающихся по контрольным вопросам, защита отчетов по практическим заданиям, тестирование
		ОК 02	**Знать:** номенклатуру информационных источников применяемых в профессиональной деятельности; **Уметь:** определять задачи поиска информации;	
		ОК 09	**Знать:** порядок применения информационных технологий и программного обеспечения в профессиональной деятельности; **Уметь:** использовать современное программное обеспечение;	
		ОК 10	**Знать:** особенности произношения; правила чтения текстов профессиональной направленности; **Уметь:** кратко обосновывать и объяснить свои действия (текущие и планируемые);	
		ПК 3.3	**Знать:** структуру и условия формирования технических каналов утечки информации; **Уметь:** применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных; **Иметь практический опыт:** проведения измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации;	

		ПК 3.4	**Знать:** номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам; **Уметь:** применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных; **Иметь практический опыт:** выявления технических каналов утечки информации;	
Раздел 5. Применение и эксплуатация технических средств защиты информации	Тема 5.1. Применение технических средств защиты информации Тема 5.2. Эксплуатация технических средств защиты информации	ОК 01	**Знать:** порядок оценки результатов решения задач профессиональной деятельности; **Уметь:** оценивать результат и последствия своих действий (самостоятельно или с помощью наставника);	опрос обучающихся по контрольным вопросам, защита отчетов по практическим заданиям, тестирование
		ОК 02	**Знать:** приемы структурирования информации; **Уметь:** оценивать практическую значимость результатов поиска; оформлять результаты поиска;	
		ОК 04	**Знать:** психологию коллектива; психологию личности; основы проектной деятельности; **Уметь:** организовывать работу коллектива и команды; взаимодействовать с коллегами, руководством, клиентами;	
		ОК 09	**Знать:** современные средства и устройства информатизации; **Уметь:** применять средства информационных технологий для решения профессиональных задач;	
		ОК 10	**Знать:** правила построения простых и сложных предложений на профессиональные темы; **Уметь:** писать простые связные сообщения на знакомые или интересующие профессиональные темы;	
		ПК 3.1	**Знать:** порядок технического обслуживания технических средств защиты информации; номенклатуру применяемых	

			средств защиты информации от несанкционированной утечки по техническим каналам; **Уметь:** применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных; **Иметь практический опыт:** установки, монтажа и настройки технических средств защиты информации; технического обслуживания технических средств защиты информации; применения основных типов технических средств защиты информации;	
		ПК 3.2	**Знать:** физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации; порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации; методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации; номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам; **Уметь:** применять технические средства для криптографической защиты информации конфиденциального характера; применять технические средства для уничтожения информации и носителей информации; применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами; **Иметь практический опыт:** применения основных	

			типов технических средств защиты информации; выявления технических каналов утечки информации; участия в мониторинге эффективности технических средств защиты информации; диагностики, устранения отказов и неисправностей, восстановления работоспособности технических средств защиты информации;	
		ПК 3.3	**Знать:** номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации; **Уметь:** применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных; **Иметь практический опыт:** проведения измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации;	
		ПК 3.4	**Знать:** основные принципы действия и характеристики технических средств физической защиты; основные способы физической защиты объектов информатизации; номенклатуру применяемых средств физической защиты объектов информатизации; **Уметь:** применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом; применять инженерно-технические средства физической защиты объектов информатизации; **Иметь практический опыт:** установки, монтажа и	

			настройки, технического обслуживания, диагностики, устранения отказов и неисправностей, восстановления работоспособности инженерно-технических средств физической защиты;	

1.2 Типовые контрольные задания или иные материалы

Текущий контроль успеваемости и промежуточная аттестация обучающихся могут проводиться как при непосредственном взаимодействии педагогического работника с обучающимися, так и с использованием ресурсов ЭИОС КузГТУ, в том числе синхронного и (или) асинхронного взаимодействия посредством сети «Интернет».

1.2.1 Оценочные средства при текущем контроле

Текущий контроль по темам дисциплины заключается в опросе обучающихся по контрольным вопросам и (или) тестировании, и (или) практических работ (при наличии).

При проведении текущего контроля обучающимся письменно, либо устно необходимо ответить на 2 вопроса, выбранных случайным.

ПРИМЕРНЫЕ ВОПРОСЫ:

Критерии оценивания при текущем контроле:

- 85–100 баллов – при правильном и полном ответе на два вопроса;
- 65–84 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 25–64 баллов – при правильном и неполном ответе только на один из вопросов;
- 0–24 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0-24	25-64	65-84	85-100
Школа оценивания	2	3	4	5

Например вопросы:

Вопрос	Ответ
1. Как называется защищенность информационной системы от случайного или преднамеренного вмешательства, наносящего ущерб владельцам или пользователям информации? а) Информационная защита информации б) Информационная безопасность в) Зашита информации	B
2. Как называется метод физического преграждения пути злоумышленнику к защищаемой информации (сигнализация, замки и т.д.)? а) Препятствие б) Управление доступом в) Маскировка	A
3. Какой метод защиты информации связан с регулированием использования всех ресурсов информационной системы? а) Маскировка б) Препятствие в) Управление доступом	C
4. Как называется установления подлинности объекта по предъявленному им идентификатору (имени)? а) Аутентификация б) Идентификация в) Маскировка	A

ПРИМЕРНОЕ ТЕСТИРОВАНИЕ

Тестирование включает как тесты с выбором ответа, так и задачи с вычисляемым ответом. Последний тип заданий формируется таким образом, чтобы верное решение задания демонстрировало владение материалом курса, но не требовало сложных вычислений. За час обучающийся должен ответить на 10 вопросов теста. Тест формируется таким образом, чтобы охватывать все темы, изучаемые в семестре, а вопрос по каждой теме попадает в тест случайным образом. Каждый верный ответ оценивается в 10 баллов.

Критерии оценивания:

90-100 баллов – при правильном ответе на 90-100%.
80-89 баллов – при правильном ответе на 80-89 %.
60-79 балла – при правильном ответе на 60-79 %.
0-59 баллов – при правильном ответе на менее 59 %.

Количество баллов	0-59	60-79	80-89	90-100
Шкала оценивания	2	3	4	5

Пример тестирования:

Вопрос	Ответ
5. Как называется метод защиты информации в информационной системе организации путем ее криптографического закрытия?	c

а) Аутентификация б) Идентификация в) Маскировка	
6. При использовании какого метода защиты пользователи системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной и уголовной ответственности? а) Принуждение б) Маскировка в) Идентификация	A
7. Какой метод защиты информации мотивирует сотрудников не нарушать установленные правила за счет соблюдения сложившихся моральных и этических норм? а) Принуждение б) Побуждение в) Маскировка	B
8. Какие средства защиты информации предназначены для внешней охраны территории объектов и защиты компонентов информационной системы организации? а) Аппаратные б) Программные в) Физические	C

1.2.2 Оценочные средства при промежуточной аттестации

Формой промежуточной аттестации является **дифференцированный зачёт (зачёт с оценкой) в 5 семестре,** в процессе которого определяется сформированность обозначенных в рабочей программе компетенций.

Зачет с оценкой проводится либо в форме опроса по контрольным вопросам, либо в форме компьютерного тестирования.

Опрос по контрольным вопросам

Во время опроса по контрольным вопросам обучающимся задается два вопроса выбранных случайным образом.

Критерии оценивания

- 85–100 баллов – при правильном и полном ответе на два вопроса;
- 65–84 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 25–64 баллов – при правильном и неполном ответе только на один из вопросов;
- 0–24 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0-24	25-64	65-84	85-100
Школа оценивания	2	3	4	5

Например вопросы:

Вопрос	Ответ
9. Какие средства защиты информации встроены в блоки информационной системы (сервера, компьютеры и т.д.) и предназначены для внутренней защиты элементов вычислительной техники и средств связи?	Аппаратные
10. Какие средства защиты информации предназначены для выполнения функций защиты информационной системы с помощью программных средств?	Физические
11. Какие средства защиты информации регламентируют правила использования, обработки и передачи информации и устанавливают меры ответственности?	Законодательные средства
12. Как называется состояние информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно?	Доступность

ПРИМЕРНОЕ ТЕСТИРОВАНИЕ

Тестирование включает как тесты с выбором ответа, так и задачи с вычисляемым ответом. Последний тип заданий формируется таким образом, чтобы верное решение задания демонстрировало владение материалом курса, но не требовало сложных вычислений. За час обучающийся должен ответить на 10 вопросов теста. Тест формируется таким образом, чтобы охватывать все темы, изучаемые в семестре, а вопрос по каждой теме попадает в тест случайным образом. Каждый верный ответ оценивается в 10 баллов.

Критерии оценивания:

90-100 баллов – при правильном ответе на 90-100%.

80-89 баллов – при правильном ответе на 80-89 %.
60-79 балла – при правильном ответе на 60-79 %.
0-59 баллов – при правильном ответе на менее 59 %.

Количество баллов	0-59	60-79	80-89	90-100
Шкала оценивания	2	3	4	5

Вопрос	Ответ
13. Какие средства защиты информации предназначены для выполнения функций защиты информационной системы с помощью программных средств? а) Аппаратные б) Программные в) Физические	В
14. Как называются правила и нормы поведения сотрудников в коллективе, регулирующие вопросы защиты информации? а) Организационные средства б) Аппаратно-программные в) Морально-этические средства	С
15. Как называется защищенность информационной системы от случайного или преднамеренного вмешательства, наносящего ущерб владельцам или пользователям информации? а) Информационная защита информации б) Информационная безопасность в) Зашита информации	В
16. Как называется метод физического преграждения пути злоумышленнику к защищаемой информации (сигнализация, замки и т.д.)? а) Препятствие б) Управление доступом в) Маскировка	А

Оценочные средства для формирования компетенции
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
Задания закрытого типа

Вопрос	Ответ
17.Информация это - а. сведения, поступающие от СМИ б. только документированные сведения о лицах, предметах, фактах, событиях в. сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления г. только сведения, содержащиеся в электронных базах данных	в
18. Информация а. не исчезает при потреблении б. становится доступной, если она содержится на материальном носителе в. подвергается только "моральному износу"	а, б, в
19. Информация, зафиксированная на материальном носителе, с реквизитами, позволяющими ее идентифицировать, называется **а. достоверной** **б. конфиденциальной** **в. документированной** **г. коммерческой тайной**	в
20. Документы, содержащие государственную тайну снабжаются грифом а. «секретно» б. «совершенно секретно» в. «особой важности»	а, б, в
21. По принадлежности информационные ресурсы подразделяются на а. государственные, коммерческие и личные	а

6. государственные, не государственные и информацию о гражданах в. информацию юридических и физических лиц г. официальные, гражданские и коммерческие	

Задания открытого типа

Вопрос	Ответ
22. Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработки информации называется:	аудиоперехват
23. По доступности информация классифицируется на:	информацию с ограниченным доступом и общедоступную информацию
24. К конфиденциальной информации относятся документы, содержащие:	государственную тайну
25. Перехват, который основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций называется:	пассивный перехват
26. К конфиденциальной информации не относится:	«ноу-хау»

Оценочные средства для формирования компетенции
ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности
Задания закрытого типа

Вопрос	Ответ
27. Вопросы информационного обмена регулируются (...) правом а. гражданским б. информационным в. конституционным г. уголовным	а
28. Система защиты государственных секретов определяется Законом а. «Об информации, информатизации и защите информации» б. «Об органах ФСБ» в. «О государственной тайне» г. «О безопасности»	в
29. Конфиденциальная информация это **а. сведения, составляющие государственную тайну** **б. сведения о состоянии здоровья высших должностных лиц** **в. документированная информация, доступ к которой ограничивается в** **г. соответствии с законодательством РФ** **д. данные о состоянии преступности в стране**	в
30. Какая информация подлежит защите? а. информация, циркулирующая в системах и сетях связи б. зафиксированная на материальном носителе информация с реквизитами, в. позволяющими ее идентифицировать г. только информация, составляющая государственные информационные ресурсы д. любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу	д
31. Государственные информационные ресурсы не могут принадлежать а. физическим лицам	а б в

б. коммерческим предприятиям в. негосударственным учреждениям	

Задания открытого типа

Вопрос	Ответ
32. Классификация и виды информационных ресурсов определены:	Законом «Об информации, информатизации и защите информации»
33. Запрещено относить к информации с ограниченным доступом	законодательные акты
34. Действие Закона «О государственной тайне» распространяется	на всех граждан и должностных лиц, если им предоставили для работы закрытые сведения
35. Перехват, который осуществляется путем использования оптической техники называется	видеоперехват
36. Что является входами системы защиты информации?	внешние и внутренние угрозы

Оценочные средства для формирования компетенции

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.

Задания закрытого типа

Вопрос	Ответ
37. Кто является основным ответственным за определение уровня классификации информации? A. Руководитель среднего звена B. Высшее руководство C. Владелец D. Пользователь	C
38. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности? A. Сотрудники B. Хакеры C. Атакующие D. Контрагенты (лица, работающие по договору)	A
39. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству? A. Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования B. Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации C. Улучшить контроль за безопасностью этой информации D. Снизить уровень классификации этой информации	C
40. Что самое главное должно продумать руководство при классификации данных? A. Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным B. Необходимый уровень доступности, целостности и конфиденциальности C. Оценить уровень риска и отменить контрмеры D. Управление доступом, которое должно защищать данные	B
41. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены? A. Владельцы данных B. Пользователи C. Администраторы D. Руководство	D

Задания открытого типа

Вопрос	Ответ
42. Что такое процедура?	Пошаговая инструкция по выполнению задачи
43. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?	Поддержка высшего руководства
44. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?	Когда стоимость контрмер превышает ценность актива и потенциальные потери
45. Что такое политики безопасности?	Широкие, высокоуровневые заявления руководства
46. Какая из приведенных техник является самой важной при выборе конкретных защитных мер?	Анализ затрат / выгоды

Оценочные средства для формирования компетенции
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
Задания закрытого типа

Вопрос	Ответ
47. Что лучше всего описывает цель расчета ALE? A. Количественно оценить уровень безопасности среды B. Оценить возможные потери для каждой контрмеры C. Количественно оценить затраты / выгоды D. Оценить потенциальные потери от угрозы в год	D
48. Тактическое планирование – это: A. Среднесрочное планирование B. Долгосрочное планирование C. Ежедневное планирование D. Планирование на 6 месяцев	
49. Что является определением воздействия (exposure) на безопасность? **A. Нечто, приводящее к ущербу от угрозы** **B. Любая потенциальная опасность для информации или систем** **C. Любой недостаток или отсутствие информационной безопасности** **D. Потенциальные потери от угрозы**	A
50. Эффективная программа безопасности требует сбалансированного применения: A. Технических и нетехнических методов B. Контрмер и защитных механизмов C. Физической безопасности и технических средств защиты D. Процедур безопасности и шифрования	A
51. Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют: A. Внедрение управления механизмами безопасности B. Классификацию данных после внедрения механизмов безопасности C. Уровень доверия, обеспечиваемый механизмом безопасности D. Соотношение затрат / выгод	C

Задания открытого типа

Вопрос	Ответ
52. Что является выходами системы защиты информации?	средства и методы защиты

53. Как называется совокупность условий и факторов, создающих потенциальную угрозу или реально существующую опасность нарушения безопасности информации?	угроза
54. Как называется попытка реализации угрозы?	атака
55. Непосредственная причина возникновения угрозы называется:	источник угрозы
56. Как называется состояние информации, при котором доступ к ней могут осуществить только субъекты, имеющие на него право?	конфиденциальность

Оценочные средства для формирования компетенции
ОК 09. Использовать информационные технологии в профессиональной деятельности.
Задания закрытого типа

Вопрос	Ответ
57. Что такое CobiT и как он относится к разработке систем информационной безопасности и программ безопасности? A. Список стандартов, процедур и политик для разработки программы безопасности B. Текущая версия ISO 17799 C. Структура, которая была разработана для снижения внутреннего мошенничества в компаниях D. Открытый стандарт, определяющий цели контроля	D
58. Что представляет собой стандарт ISO/IEC 27799? A. Стандарт по защите персональных данных о здоровье B. Новая версия BS 17799 C. Определения для новой серии ISO 27000 D. Новая версия NIST 800-60	A
59. CobiT был разработан на основе структуры COSO. Что является основными целями и задачами COSO? A. COSO – это подход к управлению рисками, который относится к контрольным объектам и бизнес-процессам B. COSO относится к стратегическому уровню, тогда как CobiT больше направлен на операционный уровень C. COSO учитывает корпоративную культуру и разработку политик D. COSO – это система отказоустойчивости	B
60. OCTAVE, NIST 800-30 и AS/NZS 4360 являются различными подходами к реализации управления рисками в компаниях. В чем заключаются различия между этими методами? A. NIST и OCTAVE являются корпоративными B. NIST и OCTAVE ориентирован на ИТ C. AS/NZS ориентирован на ИТ D. NIST и AS/NZS являются корпоративными	B
61. Какой из следующих методов анализа рисков пытается определить, где вероятнее всего произойдет сбой? A. Анализ связующего дерева B. AS/NZS C. NIST D. Анализ сбоев и дефектов	D

Задания открытого типа

Вопрос	Ответ

62. Что было разработано, чтобы помочь странам и их правительствам построить законодательство по защите персональных данных похожим образом?	OECD
63. Символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста, это метод:	Перестановки
64. Символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов, это метод:	Гаммирования
65. Как называется состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право?	Целостность
66. Спам распространяет поддельные сообщения от имени банков или финансовых компаний, целью которых является сбор логинов, паролей и пин-кодов пользователей:	Фишинг

Оценочные средства для формирования компетенции
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.
Задания закрытого типа

Вопрос	Ответ
67.Формирование политики безопасности организации относится к: 1. правовым мерам обеспечения безопасности 2. организационным мерам обеспечения безопасности 3. техническим мерам обеспечения безопасности 4. морально-этическим мерам обеспечения безопасности	**2**
68. Регламентация доступа сотрудников к защищаемым ресурсам относится к: (1) организационным мерам обеспечения безопасности (2) техническим мерам обеспечения безопасности (3) морально-этическим мерам обеспечения безопасности (4) физическим мерам обеспечения безопасности	**1**
69.Установка аппаратного межсетевого экрана относится к: (1) организационным мерам обеспечения безопасности (2) техническим мерам обеспечения безопасности (3) морально-этическим мерам обеспечения безопасности (4) физическим мерам обеспечения безопасности	**2**
70. Доктрина информационной безопасности относится к: (1) ГОСТам (2) нормативно-методическим документам (3) международным стандартам	**4**

(4) концептуальным документам	
71. К какому типу угроз в соответствии с Доктриной информационной безопасности можно отнести несанкционированный доступ к персональной информации? (1) угрозы информационному обеспечению государственной политики России (2) угрозы развитию российской индустрии информации (3) угрозы безопасности информационных и телекоммуникационных средств и систем (4) угрозы конституционным правам и свободам человека и гражданина, индивидуальному, групповому и общественному сознаниям, духовному возрождению России	**4**

Задания открытого типа

Вопрос	Ответ
72. К какому типу документов можно отнести “Положение об обеспечении безопасности конфиденциальной информации”, изданное в рамках конкретной организации?	организационный документ
73. Какие из приведенных ниже документов можно отнести к организационным?	Уставы, инструкции
74. Какие типы ИС существуют	Специальные, типовые
75. Что такое ИСПДн?	Информационная система персональных данных
76. Какие степени секретности сведений, составляющих государственную тайну, существуют?	особой важности, совершенно секретно, секретно

Оценочные средства для формирования компетенции

ПК 3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.

Задания закрытого типа

Вопрос	**Ответ**
77. К правовым методам, обеспечивающим информационную безопасность, относятся: 1.Разработка аппаратных средств обеспечения правовых данных 2. Разработка и установка во всех компьютерных правовых сетях журналов учета действий 3. Разработка и конкретизация правовых нормативных актов обеспечения безопасности	**3**
78. Основными источниками угроз информационной безопасности являются все указанное в списке: 1.Хищение жестких дисков, подключение к сети, инсайдерство 2. Перехват данных, хищение данных, изменение архитектуры системы 3. Хищение данных, подкуп системных администраторов, нарушение регламента работы	**2**
79. Виды информационной безопасности: 1.Персональная, корпоративная, государственная 2. Клиентская, серверная, сетевая 3. Локальная, глобальная, смешанная	**1**

80. Цели информационной безопасности – своевременное обнаружение, предупреждение: 1. несанкционированного доступа, воздействия в сети 2. инсайдерства в организации 3. чрезвычайных ситуаций	**1**
81. Основные объекты информационной безопасности: 1. Компьютерные сети, базы данных 2. Информационные системы, психологическое состояние пользователей 3. Бизнес-ориентированные, коммерческие системы	**1**

Задания открытого типа

Вопрос	Ответ
82. Основными рисками информационной безопасности являются:	Потеря, искажение, утечка информации
83. К основным принципам обеспечения информационной безопасности относится:	Экономической эффективности системы безопасности
84. Основными субъектами информационной безопасности являются:	органы права, государства, бизнеса
85. К основным функциям системы безопасности можно отнести все перечисленное:	Установление регламента, аудит системы, выявление рисков
86.К основным типам средств воздействия на компьютерную сеть относится:	Логические закладки («мины»)

Оценочные средства для формирования компетенции

ПК 3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации

Задания закрытого типа

Вопрос	**Ответ**
87. Когда получен спам по e-mail с приложенным файлом, следует: 1. Прочитать приложение, если оно не содержит ничего ценного – удалить 2. Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама 3. Удалить письмо с приложением, не раскрывая (не читая) его	**3**
88. Принцип Кирхгофа: 1. Секретность ключа определена секретностью открытого сообщения 2. Секретность информации определена скоростью передачи данных 3. Секретность закрытого сообщения определяется секретностью ключа	**3**
89. ЭЦП – это: 1. Электронно-цифровой преобразователь 2. Электронно-цифровая подпись 3. Электронно-цифровой процессор	**2**
90. Наиболее распространены угрозы информационной безопасности корпоративной системы: 1. Покупка нелицензионного ПО 2. Ошибки эксплуатации и неумышленного изменения режима работы системы 3. Сознательного внедрения сетевых вирусов	**2**
91. Наиболее распространены угрозы информационной безопасности сети:	**3**

1. Распределенный доступ клиент, отказ оборудования 2. Моральный износ сети, инсайдерство 3. Сбой (отказ) оборудования, нелегальное копирование данных	

Задания открытого типа

Вопрос	Ответ
92. Угроза информационной системе (компьютерной сети) – это:	Вероятное событие
93. Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:	Защищаемой
94. Окончательно, ответственность за защищенность данных в компьютерной сети несет:	Владелец сети
95. Создание и использование средств опасного воздействия на информационные сферы других стран мира и нарушение нормального функционирования информационных и телекоммуникационных систем это….	информационная война
96.Гарантия того, что АС ведет себя в нормальном и внештатном режиме так, как запланировано	надежность

Оценочные средства для формирования компетенции

ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа.

Задания закрытого типа

Вопрос	**Ответ**
97.Способность системы к целенаправленному приспособлению при изменении структуры, технологических схем или условий функционирования, которое спасает владельца АС от необходимости принятия кардинальных мер по полной замене средств защиты на новые. 1.принцип системности 2. принцип комплексности 3. принцип непрерывной защиты 4.принцип разумной достаточности 5.принцип гибкости системы	**5**
98. В классификацию вирусов по способу заражения входят 1. опасные 2. файловые 3. резидентные 4. загрузочные 5. файлово-загрузочные 6. нерезидентные	**3 6**
99. Комплекс превентивных мер по защите конфиденциальных данных и информационных процессов на предприятии это… 1. комплексное обеспечение ИБ 2. безопасность АС 3. угроза ИБ 4. атака на АС 5. политика безопасности	**1**
100.Вирусы, не связывающие свои копии с файлами, а создающие свои копии на дисках, не изменяя других файлов, называются: 1. компаньон - вирусами 2. черви 3. паразитические 4. студенческие 5. призраки 6. стелс - вирусы	**2**

7. макровирусы	
101. К видам системы обнаружения атак относятся : 1. системы, обнаружения атаки на ОС 2. системы, обнаружения атаки на конкретные приложения 3. системы, обнаружения атаки на удаленных БД **4.** все варианты верны	**4**

Задания открытого типа

Вопрос	Ответ
102. Некоторое секретное количество информации, известное только пользователю и парольной системе, которое может быть запомнено пользователем и предъявлено для прохождения процедуры аутентификации это ….	пароль пользователя
103. К вирусам изменяющим среду обитания относятся:	полиморфные
104. Охрана персональных данных, государственной служебной и других видов информации ограниченного доступа это…	Защита информации
105. Набор аппаратных и программных средств для обеспечения сохранности, доступности и конфиденциальности данных:	Компьютерная безопасность
106. Средства уничтожения, искажения или хищения информационных массивов, добывания из них необходимой информации после преодоления систем защиты, ограничения или воспрещения доступа к ним это:	информационное оружие

Оценочные средства для формирования компетенции

ПК 3.4. Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.

Задания закрытого типа

Вопрос	Ответ
107. К видам системы обнаружения атак относятся : 1. системы, обнаружения атаки на ОС 2. системы, обнаружения атаки на конкретные приложения 3. системы, обнаружения атаки на удаленных БД **4.** все варианты верны	**4**
108. Автоматизированная система должна обеспечивать 1. надежность 2. доступность 3. целостность **4.** контролируемость	**2 3**
109. Основными компонентами парольной системы являются 1. интерфейс администратора 2. хранимая копия пароля 3. база данных учетных записей 4. все варианты верны	**1 3**
110. К принципам информационной безопасности относятся 1. скрытость 2. масштабность 3. системность 4. законность **5.** открытости алгоритмов	**3 4 5**
111. Система физической безопасности включает в себя следующие подсистемы: 1. оценка обстановки 2. скрытность 3. строительные препятствия **4.** аварийная и пожарная сигнализация	**1 3 4**

Задания открытого типа

Вопрос	Ответ
112. Информация позволяющая ее обладателю при существующих или возможных обстоятельствах увеличивать доходы, сохранить положение на рынке товаров, работ или услуг это:	коммерческая тайна
113. Антивирусная программа принцип работы, которой основан на проверке файлов, секторов и системной памяти и поиске в них известных и новых вирусов называется:	Сканер
114. Что не относится к информационной инфекции:	Фальсификация данных
115. Исследование возможности расшифрования информации без знания ключей:	криптоанализ
116.Вся накопленная информация об окружающей нас дейст вительности, зафиксированная на материальных носителях или в любой другой форме, обеспечивающая ее передачу во времени и пространстве между различными потребителями для решения научных, производст венных, управленческих и других задач	Информационные ресурсы

1.2.3 Методические материалы, определяющие процедуры оценивания знаний, умений, практического опыта деятельности, характеризующие этапы формирования компетенций

Порядок организации проведения текущего контроля и промежуточной аттестации представлен в Положении о проведении текущего контроля и промежуточной аттестации обучающихся, осваивающих образовательные программы среднего профессионального образования в КузГТУ (Ип 06/10)