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: 4B52DFD6B51FDA26ACBAF4AD87221F25
Владелец: Евсина Татьяна Алексеевна
Действителен: с 01.02.2024 до 26.04.2025

УТВЕРЖДАЮ
заместитель директора по УР,
совмещающая обязанности по должности
директора филиала КузГТУ
в г. Новокузнецке
_____ Т.А. Евсина
«27» июня 2024 г.

Фонд оценочных средств дисциплины

МДК 03.01 Техническая защита информации

Специальность
«10.02.05 Обеспечение информационной безопасности автоматизированных систем»

Присваиваемая квалификация
«Техник по защите информации»

Форма обученияочная

Год набора 2022

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

Новокузнецк 2024 г.

1. Фонд оценочных средств для проведения текущего контроля, промежуточной аттестации обучающихся по дисциплине МДК 03.01 Техническая защита информации

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

1.2.2 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)

2. Задания по разделам дисциплины МДК 03.01 Техническая защита информации

Раздел 1. Концепция инженерно- техническойзащиты информации
ОК-01, ОК-02, ОК-03, 0К-09, ОК-10

Типы заданий и диагностические задания	Эталонные ответы
Задания закрытого типа	
Задание 1. *Прочитайте текст, выберите один правильный ответ* Информация а. не исчезает при потреблении б. становится доступной, если она содержится на материальномносителе в. подвергается только "моральному износу" г. Все ответы верны	г
Задание 2. *Прочитайте текст, выберите один правильный ответ* Информация, зафиксированная на материальномносителе, с реквизитами, позволяющими ее идентифицировать, называется а. достоверной б. конфиденциальной в. документированной г. коммерческой тайной	в
Задание 3. *Прочитайте текст, выберите один правильный ответ* По принадлежности информационные ресурсыподразделяются на а. государственные, коммерческие и личные 6. государственные, не государственные и информацию о гражданах в. информацию юридических и физических лиц г. официальные, гражданские и коммерческие	а
Задания открытого типа	
Задание 4. *Прочитайте текст и ответьте на вопрос* Как называется совокупность условий и факторов, создающих потенциальную угрозу или реально существующую опасность нарушения безопасности информации?	Угроза
Задание 5. *Прочитайте текст и дополните ответ* Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработкиинформации называется_____	Аудиоперехват
Задание 6. *Прочитайте текст и ответьте на вопрос* Какие средства защиты информации встроены в блоки информационной системы (сервера, компьютеры и т.д.) и	Аппаратные

предназначены для внутренней защиты элементов вычислительной техники и средств связи?	
Задание 7. *Прочитайте текст и дополните ответ* Конфиденциальной информацииотносятся документы, содержащие _____.	Государственную тайну
Задание 8. *Прочитайте текст и дополните ответ* Перехват, который основан на фиксации электромагнитныхизлучений, возникающих при функционировании средств компьютерной техники и коммуникаций называется _____ перехват.	Пассивный
Задание 9. *Прочитайте текст и дополните ответ* Символы шифруемого текста перемещаются по определеннымправилам внутри шифруемого блока этого текста, это метод _____	Перестановки
Задание 10. *Прочитайте текст и ответьте на вопрос* Как называется состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляетсятолько преднамеренно субъектами, имеющими на него право?	Целостность

Раздел 2. Теоретическиеосновы инженерно- техническойзащиты информации
ОК-01, ОК-02, ОК-03, 0К-09, ОК-10

Типы заданий и диагностические задания	Эталонные ответы
Задания закрытого типа	
Задание 1. *Прочитайте текст, выберите один правильный ответ* Какая информация подлежит защите? а. информация, циркулирующая в системах и сетях связи б. зафиксированная на материальном носителе информация среквизитами, 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
Задание 2. *Прочитайте текст, выберите один правильный ответ* Регламентация доступа сотрудников к защищаемымресурсам относится к: а. организационным мерам обеспечения безопасности б. техническим мерам обеспечения безопасности	**а**

в. морально-этическим мерам обеспечения безопасности г. физическим мерам обеспечения безопасности	
Задание 3. *Прочитайте текст, выберите один правильный ответ* Установка аппаратного межсетевого экрана относится к: а. организационным мерам обеспечения безопасности б. техническим мерам обеспечения безопасности в. морально-этическим мерам обеспечения безопасности г. физическим мерам обеспечения безопасности	б
Задание 4. *Прочитайте текст, выберите один правильный ответ* К какому типу угроз в соответствии с Доктриной информационной безопасности можно отнести несанкционированный доступ к персональной информации? а. угрозы информационному обеспечению государственной политики России б. угрозы развитию российской индустрии информации в. угрозы безопасности информационных и телекоммуникационных средств и систем г. угрозы конституционным правам и свободам человека и гражданина, индивидуальному, групповому и общественному сознаниям, духовному возрождению России	г
Задания открытого типа	
Задание 5. *Прочитайте текст и дополните ответ* Если граждане и должностные лица работают с закрытыми сведениями то на них распространяется федеральный закон «_____»	О государственной тайне
Задание 6. *Прочитайте текст и дополните ответ* Перехват, который осуществляется путем использования оптической техники называется _____	Видеоперехват
Задание 7. *Прочитайте текст и дополните ответ* Пошаговая инструкция по выполнению задач называется _____	Процедура
Задание 8. *Прочитайте текст и ответьте на вопрос* Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?	Поддержка руководства
Задание 9. *Прочитайте текст и ответьте на вопрос* Как называется метод физического преграждения пути	Препятствие

злоумышленнику к защищаемой информации (сигнализация,замки и т.д.)?	
Задание 10. *Прочитайте текст и ответьте на вопрос* Как называется попытка реализации угрозы?	Атака

Раздел 3. Физические основы технической защиты информации
ОК-01, ОК-02, 0К-09, ОК-10
ПК-3.3, ПК-3.4

Типы заданий и диагностические задания	Эталонные ответы
Задания закрытого типа	
Задание 1. *Прочитайте текст, выберите один правильный ответ* Основными источниками угроз информационной безопасности являются все указанное в списке: а. Хищение жестких дисков, подключение к сети, инсайдерство б. Перехват данных, хищение данных, изменение архитектуры системы в. Хищение данных, подкуп системных администраторов, нарушение регламента работы	б
Задание 2. *Прочитайте текст, выберите один правильный ответ* Виды информационной безопасности: а. Персональная, корпоративная, государственная б. Клиентская, серверная, сетевая в. Локальная, глобальная, смешанная г.	а
Задание 3. *Прочитайте текст, выберите один правильный ответ* Цели информационной безопасности –своевременное обнаружение, предупреждение: а. несанкционированного доступа, воздействия в сети б. инсайдерства в организации в. чрезвычайных ситуаций г.	а
Задание 4. *Прочитайте текст, выберите один правильный ответ* Основные объекты информационной безопасности: а. Компьютерные сети, базы данных б. Информационные системы, психологическое состояние пользователей в. Бизнес-ориентированные, коммерческие системы г.	а
Задания открытого типа	
Задание 5. *Прочитайте текст и дополните ответ*	Источник угрозы

Непосредственная причина возникновения угрозы называется: _____	
Задание 6. *Прочитайте текст и дополните ответ* Спам распространяет поддельные сообщения от имени банков или финансовых компаний, целью которых является сбор логинов, паролей и пин-кодов пользователей _____	Фишинг
Задание 7. *Прочитайте текст и дополните ответ* Основными рисками информационной безопасностиявляются потеря, искажение и _____информации.	Утечка
Задание 8. *Прочитайте текст и дополните ответ* Основными субъектами информационнойбезопасности являются государство и _____.	Бизнес
Задание 9. *Прочитайте текст и дополните ответ* К основным типам средств воздействия накомпьютерную сеть относится_____	Логические закладки
Задание 10. *Прочитайте текст и ответьте на вопрос* Какие средства защиты информации предназначены длявыполнения функций защиты информационной системы с помощью программных средств?	Физические

Раздел 4. Системы защиты от утечки информации
ОК-01, ОК-02, 0К-09, ОК-10
ПК-3.3, ПК-3.4

Типы заданий и диагностические задания	Эталонные ответы
Задания закрытого типа	
Задание 1. *Прочитайте текст, выберите один правильный ответ* Способность системы к целенаправленномуприспособлению при изменении структуры, технологических схем или условий функционирования,которое спасает владельца АС от необходимости принятия кардинальных мер по полной замене средств защиты на новые. а. принцип системности б. принцип комплексности в. принцип непрерывной защиты г. принцип разумной достаточности д. принцип гибкости системы	д

Задание 2. *Прочитайте текст, выберите два правильных ответа* В классификацию вирусов по способу заражения входят а. опасные б. файловые в. резидентные г. загрузочные д. файлово-загрузочные е. нерезидентные	в, е
Задание 3. *Прочитайте текст, выберите один правильный ответ* Комплекс превентивных мер по защите конфиденциальных данных и информационных процессов на предприятии это… а. комплексное обеспечение ИБ б. безопасность АС в. угроза ИБ г. атака на АС д. политика безопасности	а
Задание 4. *Прочитайте текст, выберите один правильный ответ* Вирусы, не связывающие свои копии с файлами, а создающие свои копии на дисках, не изменяя других файлов, называются: а. компаньон - вирусами б. черви в. паразитические г. студенческие д. призраки е. стелс – вирусы	б
Задания открытого типа	
Задание 5. *Прочитайте текст и дополните ответ* Некоторое секретное количество информации, известное только пользователю и парольной системе, которое может быть запомнено пользователем и предъявлено для прохождения процедуры аутентификации это _____	Пароль пользователя
Задание 6. *Прочитайте текст и дополните ответ* Охрана персональных данных, государственной служебной и других видов информации ограниченного доступа это_____	Защита информации
Задание 7. *Прочитайте текст и дополните ответ* Набор аппаратных и программных средств для обеспечения	Компьютерная

сохранности, доступности и конфиденциальности данных называется _____ безопасность.	
Задание 8. *Прочитайте текст и дополните ответ* Средства уничтожения, искажения или хищения информационных массивов, добывания из них необходимой информации после преодоления систем защиты, ограничения или воспрещения доступа к ним это _____ оружие.	Информационное
Задание 9. *Прочитайте текст и дополните ответ* Угроза информационной системе (компьютерной сети) – это _____ событие	Вероятное
Задание 10. *Прочитайте текст и ответьте на вопрос* Как называется состояние информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно?	Доступность

Раздел 5. Применение и эксплуатация технических средств защиты информации
ОК-01, ОК-02, ОК-04, 0К-09, ОК-10
ПК-3.1, ПК-3.2, ПК-3.3, ПК-3.4

Типы заданий и диагностические задания	Эталонные ответы
Задания закрытого типа	
Задание 1. *Прочитайте текст, выберите один правильный ответ* Когда получен спам по e-mail с приложенным файлом, следует: а. Прочитать приложение, если оно не содержит ничего ценного – удалить б. Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама в. Удалить письмо с приложением, не раскрывая (не читая) его	в
Задание 2. *Прочитайте текст, выберите один правильный ответ* Принцип Кирхгофа: а. Секретность ключа определена секретностью открытого сообщения б. Секретность информации определена скоростью передачи данных в. Секретность закрытого сообщения определяется секретностью ключа	в
Задание 3. *Прочитайте текст, выберите один правильный ответ* Наиболее распространены угрозы информационной безопасности сети:	в

а. Распределенный доступ клиент, отказ оборудования б. Моральный износ сети, инсайдерство в. Сбой (отказ) оборудования, нелегальное копированиеданных	
Задания открытого типа	
Задание 4. *Прочитайте текст и дополните ответ* Информация позволяющая ее обладателю присуществующих или возможных обстоятельствах увеличивать доходы, сохранить положение на рынкетоваров, работ или услуг это _____	Коммерческая тайна
Задание 5. *Прочитайте текст и дополните ответ* Антивирусная программа принцип работы, которойоснован на проверке файлов, секторов и системной памяти и поиске в них известных и новых вирусов называется _____	Сканер
Задание 6. *Прочитайте текст и дополните ответ* Исследование возможности расшифрования информации без знания ключей _____	Криптоанализ
Задание 7. *Прочитайте текст и дополните ответ* Вся накопленная информация об окружающей нас действительности, зафиксированная на материальных носителях или в любой другой форме, обеспечивающаяее передачу во времени и пространстве между различными потребителями для решения научных, производственных, управленческих и других задач называется _____	Информационные ресурсы
Задание 8. *Прочитайте текст и дополните ответ* Окончательно, ответственность за защищенностьданных в компьютерной сети несет _____	Владелец сети
Задание 9. *Прочитайте текст и дополните ответ* Создание и использование средств опасного воздействия на информационные сферы других странмира и нарушение нормального функционирования информационных и телекоммуникационных систем это _____	Информационная война
Задание 10. *Прочитайте текст и дополните ответ* Гарантия того, что АС ведет себя в нормальном ивнештатном режиме так, как запланировано называется _____	Надежность