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
Инженерно-технические средства физической защиты объектов информатизации

Специальность
«10.02.05 Обеспечение информационной безопасности автоматизированных систем»

Присваиваемая квалификация
«Техник по защите информации»

Форма обучения
очная

Год набора 2023

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. Построение и основные характеристики инженерно-технических средств физической защиты	Тема 1.1. Цели и задачи физической защиты объектов информатизации Тема 1.2. Общие положения защиты информации техническими средствами	ОК 01	**Знать**: актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; **Уметь:** распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи;	опрос обучающихся по контрольным вопросам, защита отчетов по лабораторным заданиям, тестирование
		ОК 02	**Знать:** номенклатуру информационных источников применяемых в профессиональной деятельности; **Уметь:** определять задачи поиска информации; определять необходимые источники информации; планировать процесс поиска;	
		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; основные общеупотребительные глаголы (бытовая и профессиональная лексика); **Уметь:** понимать общий смысл четко произнесенных	

			высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы; участвовать в диалогах на знакомые общие и профессиональные темы;	
Раздел 2. Основные компоненты комплекса инженерно-технических средств физической защиты	Тема 2.1 Система обнаружения комплекса инженерно-технических средств физической защиты Тема 2.2. Система контроля и управления доступом Тема 2.3. Система телевизионного наблюдения Тема 2.4. Система сбора, обработки, отображения и документирования информации Тема 2.5 Система воздействия	ОК 01	**Знать:** алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; **Уметь:** выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; составить план действия; определить необходимые ресурсы; владеть актуальными методами работы в профессиональной и смежных сферах;	опрос обучающихся по контрольным вопросам, защита отчетов по лабораторным заданиям, тестирование
		ОК 02	**Знать:** приемы структурирования информации; **Уметь:** структурировать получаемую информацию; выделять наиболее значимое в перечне информации;	
		ОК 09	**Знать:** порядок их применения и программное обеспечение в профессиональной деятельности; **Уметь:** использовать современное программное обеспечение;	
		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; кратко обосновывать и объяснить свои действия (текущие и планируемые);	
Раздел 3. Применение и эксплуатация инженерно-технических средств физической защиты	Тема 3.1 Применение инженерно-технических средств физической защиты Тема 3.2. Эксплуатация инженерно-	ОК 01	**Знать:** структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности; **Уметь:** реализовать составленный план; оценивать результат и последствия своих	опрос обучающихся по контрольным вопросам, защита отчетов по лабораторным заданиям, тестирование, выполнение и защита

	технических средств физической защиты		действий (самостоятельно или с помощью наставника);	курсовой работы (проекта)
		ОК 02	**Знать:** оценивать практическую значимость результатов поиска; оформлять результаты поиска; **Уметь:** планировать процесс поиска; структурировать получаемую информацию;	
		ОК 03	**Знать:** содержание актуальной нормативно-правовой документации; современная научная и профессиональная терминология; возможные траектории профессионального развития и самообразования; **Уметь:** определять актуальность нормативно-правовой документации в профессиональной деятельности; выстраивать траектории профессионального и личностного развития;	
		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:** особенности произношения; правила чтения текстов профессиональной направленности; **Уметь:** писать простые связные сообщения на знакомые или интересующие профессиональные темы;	
		ПК 3.5	**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
Основным положением модели системы безопасности с полным перекрытием является наличие на каждом пути проникновения в систему	хотя бы одного средства безопасности
По документам ГТК количество классов защищенности СВТ от НСД к информации	6
При избирательной политике безопасности в матрице доступа объекту системы соответствует	строка
Конкретизацией модели Белла-ЛаПадула является модель политики безопасности	LWM

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
Перехват, который осуществляется путем использования оптической техники называется: 1.активный перехват; 2.пассивный перехват; 3.аудиоперехват; 4.видеоперехват; 5.просмотр мусора.	4

К внутренним нарушителям информационной безопасности относится: 1.клиенты; 2.пользователи системы; 3.посетители; 4.любые лица, находящиеся внутри контролируемой территории; 5.представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации. 6.персонал, обслуживающий технические средства. 7сотрудники отделов разработки и сопровождения ПО; 8.технический персонал, обслуживающий здание	8
Анализ протоколируемой информации с целью оперативного выявления и предотвращения нарушений режима информационной безопасности – это? 1. Протоколирование 2. Экранирование 3. Аудит	3
Хронологически упорядоченная совокупность записей результатов деятельности субъектов АС, достаточная для восстановления, просмотра и анализа последовательности действий с целью контроля конечного результата – это? 1. Политика безопасности 2. Журнал аудита 3. Регистрационный журнал	3

1.2.2 Оценочные средства при промежуточной аттестации

Формой промежуточной аттестации является **Защита КП,** в процессе которого определяется сформированность обозначенных в рабочей программе компетенций.

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
Метод управления доступом, при котором каждому объекту системы присваивается метка критичности, определяющая ценность информации, называется	мандатным
Наименее затратный криптоанализ для криптоалгоритма DES	перебор по всему ключевому пространству
Недостаток систем шифрования с открытым ключом	относительно низкая производительность
По документам ГТК самый высокий класс защищенности СВТ от НСД к информации	1

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
Какие существуют категории система IDS? 1. IDS уровня хоста и IDS уровня сети 2. IDS уровня сети и IDS уровня шлюзов	1
Какой элемент является основным в системах обнаружения вторжений? 1. Модуль анализа 2. База сигнатур 3. Модуль протоколирования	1
К какому классу межсетевых экранов относится CISCO PIX? 1. Межсетевые экраны экспертного уровня 2. Шлюзы прикладного уровня	1
Какой элемент является основным в системах обнаружения вторжений? 1. Модуль анализа 2. База сигнатур 3. Модуль протоколирования	1

Оценочные средства для формирования компетенции

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

Задания закрытого типа

Вопрос	Ответ
Что такое процедура? 1. Правила использования программного и аппаратного обеспечения в компании 2. Пошаговая инструкция по выполнению задачи 3. Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах 4. Обязательные действия	2
Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании? 1. Поддержка высшего руководства 2. Эффективные защитные меры и методы их внедрения	1

3. Актуальные и адекватные политики и процедуры безопасности 4. Проведение тренингов по безопасности для всех сотрудников	
Что такое политика безопасности? 1. Пошаговые инструкции по выполнению задач безопасности 2. Общие руководящие требования по достижению определенного уровня безопасности 3. Широкие, высокоуровневые заявления руководства 4. Детализированные документы по обработке инцидентов безопасности	3
Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют: 1. Внедрение управления механизмами безопасности 2. Классификацию данных после внедрения механизмов безопасности 3. Уровень доверия, обеспечиваемый механизмом безопасности 4. Соотношение затрат / выгод	3
Что такое IDS? 1. Система обнаружения вторжений 2. Система межсетевого экранирования 3. Система тактического планирования 4. Система протоколирования и аудита	1

Задания открытого типа

Вопрос	Ответ
Наукой, изучающей математические методы защиты информации путем ее преобразования, является ?	криптология
Основу политики безопасности составляет?	способ управления доступом
С точки зрения ГТК основной задачей средств безопасности является обеспечение?	защиты от НСД
Класс F-DC согласно «Европейским критериям» характеризуется повышенными требованиями к ….	конфиденциальности
Какая длина исходного ключа у алгоритма шифрования DES (бит)?	56

Оценочные средства для формирования компетенции

ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

Задания закрытого типа

Вопрос	Ответ
Кто сформулировал принципы обеспечения целостности? 1. Кларк и Вилсон 2. Митник и Кларк 3. Шеннон и Вилсон	1
Защита информации это: 1.процесс сбора, накопления, обработки, хранения, распределения и поиска информации;	5

2.преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа; 3.получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств; 4.совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям; 5.деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.	
Перехват, который основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций называется: 1.активный перехват; 2.пассивный перехват; 3.аудиоперехват; 4.видеоперехват;	2
Под replay-атакой понимается: 1. модификация передаваемого сообщения 2. повторное использование переданного ранее сообщения 3. невозможность получения сервиса законным пользователем	2
Уровень секретности - это 1. ответственность за модификацию и НСД информации 2. административная или законодательная мера, соответствующая мере ответственности лица за утечку или потерю конкретной секретной информации, регламентируемой специальным документом, с учетом государственных, военно-стратегических, коммерческих, служебных или частных интересов	2

Задания открытого типа

Вопрос	Ответ
Достоинствами программной реализации криптографического закрытия данных являются?	практичность и гибкость
Если средства защиты могут быть преодолены только государственной спецслужбой, то согласно "Европейским критериям" безопасность считается:	высокой
Если средство защиты способно противостоять корпоративному злоумышленнику, то согласно "Европейским критериям" безопасность считается:	средней
Если средство защиты способно противостоять отдельным атакам, то согласно "Европейским критериям" безопасность считается:	базовой
Длина исходного ключа в ГОСТ 28147-89 (бит):	256

Оценочные средства для формирования компетенции

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.
Задания закрытого типа

Вопрос	Ответ
Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработки информации называется: 1.активный перехват; 2.пассивный перехват; 3.аудиоперехват; 4.видеоперехват; 5.просмотр мусора.	3
Кто является знаковой фигурой в сфере информационной безопасности 1. Митник 2. Шеннон 3. Паскаль 4. Беббидж	1
Что было разработано, чтобы помочь странам и их правительствам построить законодательство по защите персональных данных похожим образом? 1. Безопасная OECD 2. ISO\IEC 3. OECD 4. CPTED	3
Что представляет собой стандарт ISO/IEC 27799? 1. Стандарт по защите персональных данных о здоровье 2. Новая версия BS 17799 3. Определения для новой серии ISO 27000 4. Новая версия NIST 800-60	1
Какой из следующих законодательных терминов относится к компании или человеку, выполняющему необходимые действия, и используется для определения обязательств? 1. Стандарты 2. Должный процесс (Due process) 3. Должная забота (Due care) 4. Снижение обязательств	3

Задания открытого типа

Вопрос	Ответ
Для реализации технологии RAID создается:	псевдодрайвер
Достоинством дискретных моделей политики безопасности является:	простой механизм реализации
Единственный ключ используется в криптосистемах	симметричных
Запись определенных событий в журнал безопасности сервера называется:	аудитом
Главным параметром криптосистемы является показатель	криптостойкости

Оценочные средства для формирования компетенции

ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

Задания закрытого типа

Вопрос	Ответ
Почему количественный анализ рисков в чистом виде не достижим? 1. Он достижим и используется 2. Он присваивает уровни критичности. Их сложно перевести в денежный вид. 3. Это связано с точностью количественных элементов 4. Количественные измерения должны применяться к качественным элементам	4
Если используются автоматизированные инструменты для анализа рисков, почему все равно требуется так много времени для проведения анализа? 1. Много информации нужно собрать и ввести в программу 2. Руководство должно одобрить создание группы 3. Анализ рисков не может быть автоматизирован, что связано с самой природой оценки 4. Множество людей должно одобрить данные	1
Что из перечисленного не является задачей руководства в процессе внедрения и сопровождения безопасности? 1. Поддержка 2. Выполнение анализа рисков 3. Определение цели и границ 4. Делегирование полномочий	2
Что из перечисленного не является целью проведения анализа рисков? 1. Делегирование полномочий 2. Количественная оценка воздействия потенциальных угроз 3. Выявление рисков 4. Определение баланса между воздействием риска и стоимостью необходимых контрмер	1
Что является определением воздействия (exposure) на безопасность? 1. Нечто, приводящее к ущербу от угрозы 2. Любая потенциальная опасность для информации или систем 3. Любой недостаток или отсутствие информационной безопасности 4. Потенциальные потери от угрозы	1

Задания открытого типа

Вопрос	Ответ
В многоуровневой модели, если субъект доступа формирует запрос на изменение, то уровень безопасности объекта относительно уровня безопасности субъекта должен:	доминировать

В многоуровневой модели, если субъект доступа формирует запрос на чтение-запись, то уровень безопасности субъекта относительно уровня безопасности объекта должен:	быть равен
Оконечное устройство канала связи, через которое процесс может передавать или получать данные, называется:	сокетом
Совокупность свойств, обусловливающих пригодность информации удовлетворять определенные потребности в соответствии с ее назначением, называется	качеством информации

Оценочные средства для формирования компетенции

ОК 09. Использовать информационные технологии в профессиональной деятельности.

Задания закрытого типа

Вопрос	Ответ
Что лучше всего описывает цель расчета ALE? 1. Количественно оценить уровень безопасности среды 2. Оценить возможные потери для каждой контрмеры 3. Количественно оценить затраты / выгоды 4. Оценить потенциальные потери от угрозы в год	4
Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков? 1. Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски 2. Когда риски не могут быть приняты во внимание по политическим соображениям 3. Когда необходимые защитные меры слишком сложны 4. Когда стоимость контрмер превышает ценность актива и потенциальные потери	4
Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены? 1. Владельцы данных 2. Пользователи 3. Администраторы 4. Руководство	4
Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности? 1. Сотрудники 2. Хакеры 3. Атакующие 4. Контрагенты (лица, работающие по договору)	1
Кто является основным ответственным за определение уровня классификации информации? 1. Руководитель среднего звена 2. Высшее руководство 3. Владелец 4. Пользователь	3

Задания открытого типа

Вопрос	Ответ

Конкретизацией модели Белла-ЛаПадула является модель политики безопасности	LWM
Недостатком дискретных моделей политики безопасности является	статичность
По документам ГТК количество классов защищенности АС от НСД	9
С помощью закрытого ключа информация	расшифровывается
При качественном подходе риск измеряется в терминах	заданных с помощью шкалы или ранжирования

ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.
(в ред. Приказа Минпросвещения России от 17.12.2020 N 747)
Задания закрытого типа

Вопрос	Ответ
В модели политики безопасности Лендвера ссылка на сущность, если это идентификатор сущности, называется 1.прямой 2.простой 3.циклической 4.косвенной	1
Из перечисленного: 1) администраторы; 2) пользователи; 3) задания; 4) терминалы; 5) программы; 6) файлы — модель политики безопасности Адепт-50 рассматривает следующие группы безопасности 1.2, 3, 4, 6 2.1, 2, 5, 6 3.3, 4, 5, 6 4.1, 2, 3, 4	1
Абстрактное описание системы, без связи с ее реализацией, дает модель политики безопасности 1.Белла-ЛаПадула 2.На основе анализа угроз 3.С полным перекрытием 4.Лендвера	1
Выделения пользователем и администраторам только тех прав доступа, которые им необходимы это 1.принцип минимазации привилегий 2.принцип простоты и управляемости ИС 3.принцип многоуровневой защиты 4.принцип максимизации привилегий	1
Два ключа используются в криптосистемах 1.с открытым ключом 2.двойного шифрования 3.симметричных 4.с закрытым ключом	1

Задания открытого типа

Вопрос	Ответ

Недостаток систем шифрования с открытым ключом	относительно низкая производительность
Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?	Руководство
Наименее затратный криптоанализ для криптоалгоритма RSA	разложение числа на простые множители
Недостатком дискретных моделей политики безопасности является	статичность
Нормативный документ, регламентирующий все аспекты безопасности продукта информационных технологий, называется	профилем защиты

ПК 3.5. Организовывать отдельные работы по физической защите объектов информатизации.

Задания закрытого типа

Вопрос	Ответ
Для решения проблемы правильности выбора и надежности функционирования средств защиты в «Европейских критериях» вводится понятие 1.адекватности средств защиты 2.унификации средств защиты 3.надежности защиты информации 4.оптимизации средств защиты	1
Достоинством дискретных моделей политики безопасности является 1.простой механизм реализации 2.числовая вероятностная оценка надежности 3.высокая степень надежности 4.динамичность	1
Из перечисленного: 1) анализ потенциального злоумышленника; 2) оценка возможных затрат; 3) оценка возможных потерь; 4) анализ потенциальных угроз — процесс анализа рисков при разработке системы защиты ИС включает 1.3, 4 2.2, 4 3.1, 3 4.1, 2	1
Недостатком модели политики безопасности на основе анализа угроз системе является 1.изначальное допущение вскрываемости системы 2.необходимость дополнительного обучения персонала 3.сложный механизм реализации 4.статичность	1
При избирательной политике безопасности в матрице доступа объекту системы соответствует 1.строка 2.прямоугольная область 3.ячейка 4.столбец	1

Задания открытого типа

Вопрос	Ответ
При полномочной политике безопасности совокупность меток с одинаковыми значениями образует	уровень безопасности
Проверка подлинности субъекта по предъявленному им идентификатору для принятия решения о предоставлении	аутентификация

ему доступа к ресурсам системы — это	
При качественном подходе риск измеряется в терминах	заданных с помощью шкалы или ранжирования
Количество уровней адекватности, которое определяют «Европейские критерии»	7
Математические методы нарушения конфиденциальности и аутентичности информации без знания ключей объединяет	криптоанализ

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)