

**Министерство науки и высшего образования РФ  
Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
«Национальный исследовательский университет «МЭИ»**

**Направление подготовки/специальность: 10.04.01 Информационная безопасность**

**Наименование образовательной программы: Управление информационной безопасностью**

**Уровень образования: высшее образование - магистратура**

**Форма обучения: Очная**

**Оценочные материалы  
по дисциплине  
Критерии оценки безопасности информационных технологий**

**Москва  
2022**

## ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Преподаватель

(должность)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Невский А.Ю.
	Идентификатор	R4bc65573-NevskyAY-0b6e493d

(подпись)

А.Ю.

Невский

(расшифровка  
подписи)

## СОГЛАСОВАНО:

Руководитель  
образовательной  
программы

(должность, ученая степень, ученое  
звание)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Минзов А.С.
	Идентификатор	R17801759-MinzovAS-e8de8907

(подпись)

А.С. Минзов

(расшифровка  
подписи)

Заведующий  
выпускающей кафедры

(должность, ученая степень, ученое  
звание)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Невский А.Ю.
	Идентификатор	R4bc65573-NevskyAY-0b6e493d

(подпись)

А.Ю.

Невский

(расшифровка  
подписи)

## ОБЩАЯ ЧАСТЬ

Оценочные материалы по дисциплине предназначены для оценки: достижения обучающимися запланированных результатов обучения по дисциплине, этапа формирования запланированных компетенций и уровня освоения дисциплины.

Оценочные материалы по дисциплине включают оценочные средства для проведения мероприятий текущего контроля успеваемости и промежуточной аттестации.

Формируемые у обучающегося компетенции:

1. ПК-1 Оценивание уровня безопасности компьютерных систем и сетей  
ПК-1.1 Проводит контрольные проверки работоспособности и эффективности применяемых программно-аппаратных средств защиты информации
2. ПК-2 Разработка систем защиты информации автоматизированных систем  
ПК-2.1 Тестирует системы защиты информации автоматизированных систем

и включает:

**для текущего контроля успеваемости:**

Форма реализации: Выполнение задания

1. Контрольная работа 1. Практическое применение «Общих критериев» оценки безопасности информационных технологий для разработки профилей защиты и заданий по безопасности (Контрольная работа)

Форма реализации: Защита задания

1. Защита результатов, полученных на практическом занятии №8. Защита результатов, полученных на практическом занятии №9. Защита результатов выполнения индивидуального задания: Разработка задания по безопасности для продукта информационной технологии (Индивидуальный проект)

Форма реализации: Письменная работа

1. Тест 1. Зарубежный опыт разработки критериев оценки безопасности информационных технологий (Тестирование)
2. Тест 2. Терминология и общая модель критериев оценки безопасности информационных технологий (ГОСТ Р ИСО/МЭК 15408). Защита результатов, полученных на практическом занятии №7 (Тестирование)

## БРС дисциплины

2 семестр

Раздел дисциплины	Веса контрольных мероприятий, %				
	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
	Срок КМ:	4	8	12	15
Основные требования безопасности информационных технологий.					
Подходы к разработке критериев оценки безопасности информационных технологий. (Зарубежный опыт).	+				
Стандарты серии ГОСТ Р ИСО/МЭК 15408 «Общие критерии». Систематизированные каталоги функциональных компонент безопасности и доверия к безопасности информационных					

технологий.				
Общая модель критериев оценки безопасности информационных технологий.		+	+	
Критерии оценки безопасности информационных технологий. Функциональные компоненты безопасности		+	+	
Критерии оценки безопасности информационных технологий. Компоненты доверия к безопасности.		+	+	
Практическое применение подходов «Общих» критериев при разработке задания по безопасности для конкретного класса информационных технологий.				
Практическое применение «Общих критериев» оценки безопасности информационных технологий.				+
Методология оценки безопасности информационных технологий.				+
Вес КМ:	15	20	25	40

\$Общая часть/Для промежуточной аттестации\$

## СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ТЕКУЩЕГО КОНТРОЛЯ

### *I. Оценочные средства для оценки запланированных результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций*

Индекс компетенции	Индикатор	Запланированные результаты обучения по дисциплине	Контрольная точка
ПК-1	ПК-1.1 <sub>ПК-1</sub> Проводит контрольные проверки работоспособности и эффективности применяемых программно-аппаратных средств защиты информации	<p>Знать:</p> <p>перечень, структуру, общее содержание национальных стандартов серии ГОСТ Р ИСО/МЭК 15408, а также перечень функциональных компонент безопасности и компонент доверия к безопасности информационных технологий основы методологии «Общих критериев» для практического использования при оценке безопасности информационных технологий</p> <p>Уметь:</p> <p>применять современное и эффективное средство управления безопасностью информационных технологий на основе</p>	<p>Тест 1. Зарубежный опыт разработки критериев оценки безопасности информационных технологий (Тестирование)</p> <p>Контрольная работа 1. Практическое применение «Общих критериев» оценки безопасности информационных технологий для разработки профилей защиты и заданий по безопасности (Контрольная работа)</p> <p>Тест 2. Терминология и общая модель критериев оценки безопасности информационных технологий (ГОСТ Р ИСО/МЭК 15408). Защита результатов, полученных на практическом занятии №7 (Тестирование)</p>

			использования отечественных и международных стандартов проводить обоснование перечня функциональных компонент безопасности при разработке профилей защиты и заданий по безопасности информационных технологий	
ПК-2	ПК-2.1 <sub>ПК-2</sub> Тестирует системы информации автоматизированных систем защиты		Знать: порядок, технологию и критерии оценки (оценочные уровни доверия) к безопасности информационных технологий и их сущность Уметь: выполнять в полном объеме разработку задания по безопасности для образца информационной технологии, включая нетривиальные реализации (киберфизические системы, облачные технологии, технологии больших данных и др.)	Защита результатов, полученных на практическом занятии №8. Защита результатов, полученных на практическом занятии №9. Защита результатов выполнения индивидуального задания: Разработка задания по безопасности для продукта информационной технологии (Индивидуальный проект)

## II. Содержание оценочных средств. Шкала и критерии оценивания

### КМ-1. Тест 1. Зарубежный опыт разработки критериев оценки безопасности информационных технологий

**Формы реализации:** Письменная работа

**Тип контрольного мероприятия:** Тестирование

**Вес контрольного мероприятия в БРС:** 15

**Процедура проведения контрольного мероприятия:** Письменный опрос с вариантами ответов

#### Краткое содержание задания:

Тестирование. Необходимо выбрать верный вариант ответа на вопрос.

#### Контрольные вопросы/задания:

<p>Знать: основы методологии «Общих критериев» для практического использования при оценке безопасности информационных технологий</p>	<p>1. Как называется вторая часть ОК?</p> <ol style="list-style-type: none"><li>1. Компоненты доверия к безопасности</li><li>2. Функциональные компоненты безопасности</li><li>3. Руководство по разработке заданий по безопасности</li><li>4. Руководство по разработке профилей защиты</li></ol> <p>2. Международная организация по стандартизации имеет аббревиатуру</p> <ol style="list-style-type: none"><li>1. ISO</li><li>2. IEC</li><li>3. ICSO</li><li>4. 3</li><li>5. 1 и 3</li></ol> <p>3. Стандартизацией в какой области не занимается ISO?</p> <ol style="list-style-type: none"><li>1. занимается всеми</li><li>2. электротехника и электроника</li><li>3. криптография</li><li>4. техническая защита информации</li></ol>
<p>Уметь: применять современное и эффективное средство управления безопасностью информационных технологий на основе использования отечественных и международных стандартов</p>	<p>1. Какие документы разработаны ISO для поддержки ОК?</p> <ol style="list-style-type: none"><li>1. Руководство по разработке ПЗ и ЗБ</li><li>2. Процедуры регистрации ПЗ</li><li>3. 1 и 2</li><li>4. Общая методология оценки безопасности ИТ</li><li>5. 1 и 4</li><li>6. 1, 2, 4</li></ol> <p>2. Какой разрешенной операции на компонентах нет в ОК?</p> <ol style="list-style-type: none"><li>1. Итерация</li><li>2. Повторение</li><li>3. Уточнение</li><li>4. Выбор</li><li>5. Назначение</li></ol>

**Описание шкалы оценивания:**

*Оценка: 5*

*Нижний порог выполнения задания в процентах: 70*

*Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно*

*Оценка: 4*

*Нижний порог выполнения задания в процентах: 60*

*Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач*

*Оценка: 3*

*Нижний порог выполнения задания в процентах: 50*

*Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено*

**КМ-2. Контрольная работа 1. Практическое применение «Общих критериев» оценки безопасности информационных технологий для разработки профилей защиты и заданий по безопасности**

**Формы реализации:** Выполнение задания

**Тип контрольного мероприятия:** Контрольная работа

**Вес контрольного мероприятия в БРС: 20**

**Процедура проведения контрольного мероприятия:** Проводится по заданию. Выполняется в течение 2 недель

**Краткое содержание задания:**

Используя общедоступные данные о назначении, архитектуре, компонентах, порядке взаимодействия основных из них, перечне основных режимов работы и среды функционирования, разработать перечень основных компонентов безопасности, которыми должно обладать САВЗ.

**Контрольные вопросы/задания:**

Знать: перечень, структуру, общее содержание национальных стандартов серии ГОСТ Р ИСО/МЭК 15408, а также перечень функциональных компонент безопасности и компонент доверия к безопасности информационных технологий	1. Назначение, архитектура, перечень компонентов, порядок взаимодействия основных компонентов САВЗ. 2. Перечень основных режимов работы, среда функционирования САВЗ,
Уметь: проводить обоснование перечня функциональных компонент безопасности при разработке профилей защиты и заданий по безопасности информационных технологий	1. Разработка перечень основных компонентов безопасности для САВЗ.

**Описание шкалы оценивания:**

*Оценка: 5*

*Нижний порог выполнения задания в процентах: 80*



*Описание характеристики выполнения знания:* Описание выполнено с высоким качеством

*Оценка:* 4

*Нижний порог выполнения задания в процентах:* 60

*Описание характеристики выполнения знания:* Описание выполнено с высоким и средним качеством

*Оценка:* 3

*Нижний порог выполнения задания в процентах:* 50

*Описание характеристики выполнения знания:* Описание выполнено со средним качеством

**КМ-3. Тест 2. Терминология и общая модель критериев оценки безопасности информационных технологий (ГОСТ Р ИСО/МЭК 15408). Защита результатов, полученных на практическом занятии №7**

**Формы реализации:** Письменная работа

**Тип контрольного мероприятия:** Тестирование

**Вес контрольного мероприятия в БРС:** 25

**Процедура проведения контрольного мероприятия:** Письменный опрос с вариантами ответов

**Краткое содержание задания:**

Тестирование. Необходимо выбрать верный вариант ответа на вопрос.

**Контрольные вопросы/задания:**

<p>Знать: перечень, структуру, общее содержание национальных стандартов серии ГОСТ Р ИСО/МЭК 15408, а также перечень функциональных компонент безопасности и компонент доверия к безопасности информационных технологий</p>	<p>1. Стандартизацией в какой области занимается международная организация ИЕС?</p> <ol style="list-style-type: none"><li>1. Электротехники и электроники</li><li>2. Электротехники, электроники и радиосвязи</li><li>3. Приборостроения</li><li>4. Смежных технологий</li><li>5. 1-3</li><li>6. Все перечисленные</li></ol> <p>2. Для каких структурных частей требований доверия предполагается описание ЦЕЛИ?</p> <ol style="list-style-type: none"><li>1. Класс</li><li>2. Семейство</li><li>3. Компонент</li><li>4. Элемент</li><li>5. Класс и семейство</li><li>6. Семейство и компонент</li></ol> <p>3. Какой уровень доверия предполагает полуформальную верификацию проекта и тестирование?</p> <ol style="list-style-type: none"><li>1. 2</li><li>2. 4</li><li>3. 6</li><li>4. 8</li></ol>
<p>Уметь: проводить обоснование перечня функциональных компонент безопасности при разработке профилей защиты и заданий по безопасности</p>	<p>1. Какое положение не относится к ограничениям на применение ОК?</p> <ol style="list-style-type: none"><li>1. нет критериев для административных мер;</li><li>2. не рассматривается административно-правовая структура;</li></ol>

информационных технологий	<p>3. все перечисленные относятся;</p> <p>4. нет критериев для криптографических алгоритмов;</p> <p>5. не рассматривается методология оценки;</p> <p>6. нет процедур для использования результатов оценки.</p> <p>2. В каком стандарте дается «Руководство по разработке профилей защиты и заданий по безопасности»?</p> <p>1. 13335;</p> <p>2. 15408;</p> <p>3. 57628;</p> <p>4. 18044;</p> <p>5. 27005.</p> <p>3. Что в данном примере «FDP_IFF.4.2» обозначает цифра 2?</p> <p>1. Элемент компонента;</p> <p>2. Функциональное семейство</p> <p>3. Функциональный класс;</p> <p>4. Компонент семейства.</p>
---------------------------	--

**Описание шкалы оценивания:**

*Оценка: 5*

*Нижний порог выполнения задания в процентах: 70*

*Описание характеристики выполнения знания:* Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

*Оценка: 4*

*Нижний порог выполнения задания в процентах: 60*

*Описание характеристики выполнения знания:* Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

*Оценка: 3*

*Нижний порог выполнения задания в процентах: 50*

*Описание характеристики выполнения знания:* Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

**КМ-4. Защита результатов, полученных на практическом занятии №8. Защита результатов, полученных на практическом занятии №9. Защита результатов выполнения индивидуального задания: Разработка задания по безопасности для продукта информационной технологии**

**Формы реализации:** Защита задания

**Тип контрольного мероприятия:** Индивидуальный проект

**Вес контрольного мероприятия в БРС:** 40

**Процедура проведения контрольного мероприятия:** Проводится по заданию. Выполняется в течение срока, указанного в задании

**Краткое содержание задания:**

**«Разработка задания по безопасности (ЗБ) для продукта информационной технологии Интернета вещей»**

*Введение:*

Согласно оценкам специалистов, к 2020 году свыше 50 миллиардов устройств по всему миру будут подключены к Интернету. Среди них есть устройства, выполняющие как промышленные задачи, так и многочисленные бытовые.

Совокупность таких устройств принято обозначать термином **Интернет вещей** (Internet of things, IoT) или **киберфизические объекты**.

При таком темпе роста очень критично встаёт вопрос безопасности устройств в случае отсутствия (несовершенства) процессов, обеспечивающих доступность, целостность (в ряде случаев – конфиденциальность) и шифрование данных.

*Выполнить:*

1. В должности сотрудника отдела разработки требований безопасности информационных технологий компании-интегратора «Х» на основе анализа особенностей обеспечения информационной безопасности в интересах конкретного класса устройств Интернета вещей разработать «Задание по безопасности для продукта информационной технологии Интернета вещей».

*Исходные данные для разработки:*

А) Тип (класс) устройств Интернета вещей – Объект оценки (ОО):

1. Бытовой интернет вещей;
2. Промышленный интернет вещей;
3. Устройства Smart Metering;
4. Системы и устройства видеоаналитики;
5. Системы и устройства WiFi-аналитики;
6. Системы и устройства «Умный город», «Умное жилище»;
7. Системы интеллектуальной логистики
8. Системы мониторинга состояния человека (животного, транспортного средства)

В) Оценочный уровень доверия к ОО студент определяет самостоятельно, исходя из положений [4], логики практического использования ОО, его стоимостных показателей, характера угроз и критичности последствий при нарушения механизмов защиты.

Г) В случае отсутствия разработанного профиля защиты для типа (класса) устройств Интернета вещей раздел 7 не заполняется, о чем делается запись, например, «Нет разработанного профиля защиты».

Д) Используемые источники и документы:

1. Материалы лекций по учебной дисциплине «Критерии оценки безопасности информационных технологий», 2017 г..
2. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.
3. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности.
4. ГОСТ Р ИСО/МЭК 15408-3-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности.
5. ГОСТ Р ИСО/МЭК 15446-2008 Информационная технология. Методы и средства обеспечения безопасности.. Руководство по разработке профилей защиты и заданий по безопасности..
6. РД Гостехкомиссия России, 2003 г. Безопасность информационных технологий. Положение по разработке профилей защиты и заданий по безопасности.

7. Программный комплекс UserGate Proxy & Firewall 5.2. F. Задание по безопасности UG\_P&F\_5.2.F.ЗБ, [Электронный документ], <https://www.altx-soft.ru/files/groups/260.pdf>.

*Технология выполнения задания:*

- a. Изучить настоящее задание;
- b. Тип (класс) продукта информационной технологии интернета вещей студент выбирает самостоятельно из раздела А) настоящего задания в соответствии со своим порядковым номером в списке учебной группы. Студент с порядковым номером 9 выбирает вариант №1; 10 – 2 и т.д.
- c. Конкретную технологию из соответствующего класса студент выбирает самостоятельно, например для:
  - бытового интернета вещей - интеллектуальные бытовые приборы: а) холодильник с функцией заказа продуктов и возможностью его оплаты; б) интеллектуальный пылесос (стиральная машина, кофе машина, пароварка с функцией удаленного управления и другие;
  - промышленного интернета вещей – интеллектуальная система сортировки багажа в аэропортах и другие;
  - устройства Smart Metering – системы учета потребления электро, теплоэнергии, газа, воды с функцией удаленного управления, передачи информации и оплаты услуг и другие;
  - систем и устройств видеоаналитики – интеллектуальные системы противодействия терроризму и другие;
  - систем и устройств WiFi-аналитики - интеллектуальные системы идентификации личности, состояния и поведения человека, геолокации человека и другие;
  - систем и устройств «Умный город», «Умное жилище» - интеллектуальная охранная система с функцией удаленного управления; интеллектуальная система управления дорожным (уличным) движением и другие;
  - систем интеллектуальной логистики – управление транспортными, товарными, информационными, денежными потоками с функцией самостоятельного принятия решения;
  - систем мониторинга состояния человека (животного, транспортного средства) – информеры на основе показаний частоты пульса, сердечного ритма, температуры тела, жестов, факта падения и другие.
- d. Ознакомиться с содержанием рекомендуемых документов (стандарты, РД ФСТЭК);
- e. Ознакомиться с общими характеристиками и сформировать перечень требований безопасности для выбранного объекта оценки (ОО) – класса устройств Интернета вещей;
- f. Разработать ЗБ для выбранного программного средства;
- g. Защитить ЗБ посредством ответа на вопросы руководителя по существу выполненной работы.

*Примечание:*

1. Для разработки ЗБ использовать требования стандарта ГОСТ Р ИСО/МЭК ТО 15446-2008 (раздел 7-11). Этот же материал можно найти на официальном сайте ФСТЭК - Руководящий документ. Гостехкомиссия России, 2003 год «Руководство по разработке профилей защиты и заданий по безопасности»
2. Структуру и содержание основных разделов ЗБ взять из ГОСТ Р ИСО/МЭК ТО 15446-2008 (приложение В).
3. Каждый компонент (требование) безопасности, а также (доверия к безопасности), являющееся стандартными, выбирается из соответствующих классов и семейств, описанные источниками [3,4].

4. Каждый специальный компонент (требование) безопасности, а также (доверия к безопасности), описывается студентом самостоятельно в приложениях к разработанному ЗБ.

**Контрольные вопросы/задания:**

<p>Знать: порядок, технологию и критерии оценки (оценочные уровни доверия) к безопасности информационных технологий и их сущность</p>	<p>1.Каковы ограничения на использование ОК?                  2.Как называются в ОК наборы функциональных требований безопасности для многократного использования?                  3.В каком стандарте дается «Руководство по разработке профилей защиты и заданий по безопасности»?</p>
<p>Уметь: выполнять в полном объеме разработку задания по безопасности для образца информационной технологии, включая нетривиальные реализации (киберфизические системы, облачные технологии, технологии больших данных и др.)</p>	<p>1.Какой вид зависимости в таблицах зависимостей для функциональных компонентов обозначается символом «X»?                  2.Каковы задачи оценки, сформулирован в ОМО? Их общая характеристика</p>

**Описание шкалы оценивания:**

*Оценка: 5*

*Нижний порог выполнения задания в процентах: 90*

*Описание характеристики выполнения знания:* Задание по безопасности выполнено полно (90 %) и качественно

*Оценка: 4*

*Нижний порог выполнения задания в процентах: 70*

*Описание характеристики выполнения знания:* Задание по безопасности выполнено полно (70 %) и качественно. Допускаются отдельные неточности и ошибки

*Оценка: 3*

*Нижний порог выполнения задания в процентах: 50*

*Описание характеристики выполнения знания:* Задание по безопасности выполнено недостаточно полно (50 %) и качественно. Присутствуют значительные неточности и ошибки

# СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

2 семестр

Форма промежуточной аттестации: Экзамен

Пример билета

<b>НИУ МЭИ</b>	<b>ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1</b> Кафедра <i>Безопасности и информационных технологий</i> Дисциплина <b>«КРИТЕРИИ ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ»</b>	<i>Утверждаю: Зав. каф. БИТ А.Ю.Невский</i>
		Протокол № от 2021 года
Используя любые доступные источники информации сделать подробное описание порядка разработки раздела ПЗ для САВЗ «Среда безопасности объекта оценки». В описание включить сведения: - документ, на основе которого разрабатывается раздел; - основное содержание раздела; - порядок идентификации предположений безопасности, варианты; - порядок идентификации угроз безопасности, виды угроз, варианты; - порядок идентификации политик безопасности, виды политик, варианты.		

## Процедура проведения

Письменный ответ в течении 50 минут

### *1. Перечень компетенций/индикаторов и контрольных вопросов проверки результатов освоения дисциплины*

**1. Компетенция/Индикатор:** ПК-1.1<sub>ПК-1</sub> Проводит контрольные проверки работоспособности и эффективности применяемых программно-аппаратных средств защиты информации

### **Вопросы, задания**

1. Как называется документ, на основе которого разрабатывается раздел “Требования доверия...”
2. Каков порядок формирования дополнительных компонент доверия, их виды и варианты?

### **Материалы для проверки остаточных знаний**

1. Сколько функциональных классов требований доверия к безопасности описаны в ОК-3?

Ответы:

1. 7
2. 8
3. 9
4. 10

Верный ответ: 1. 7

2. К структуре описания какого структурного элемента функциональных требований в ОК-2 относится блок «Управление»?

Ответы:

1. Функционального класса;
2. Функционального компонента;
3. Функционального семейства;
4. 1 и 2;
5. Всех перечисленных.

Верный ответ: 3. Функционального семейства

**2. Компетенция/Индикатор:** ПК-2.1<sub>ПК-2</sub> Тестирует системы защиты информации автоматизированных систем

### **Вопросы, задания**

1. Подробное описание порядка разработки раздела ПЗ для САВЗ «Требования доверия к безопасности объекта оценки»;
2. Каков порядок формирования перечня компонент доверия?;

### **Материалы для проверки остаточных знаний**

1. По каким критериям оценивается надежность информационных систем в соответствии с «оранжевой книгой» США?

Ответы:

1. Политика безопасности;
2. Методы защиты информации;
3. Гарантированность
4. 1 и 2;
5. 1 и 3
6. 1-3.

Верный ответ: 5. 1 и 3

2. Какой тип документа подготавливается по результатам оценки?

Ответы:

1. Техническое обоснование
2. Технический сертификат
3. Технический акт
4. Технический отчет
5. Техническое задание

Верный ответ: 4. Технический отчет

## **II. Описание шкалы оценивания**

*Оценка: 5*

*Нижний порог выполнения задания в процентах: 80*

*Описание характеристики выполнения знания: Все ответы правильные*

*Оценка: 4*

*Нижний порог выполнения задания в процентах: 60*

*Описание характеристики выполнения знания: все ответы правильные*

*Оценка: 3*

*Нижний порог выполнения задания в процентах: 50*

*Описание характеристики выполнения знания: все ответы правильные*

## **III. Правила выставления итоговой оценки по курсу**

Оценка определяется в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ» на основании семестровой и экзаменационной составляющих.