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	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Невский А.Ю. Идентификатор: R4bc65573-NevskyAY-0b6e493d	А.Ю. Невский
(должность)	(подпись)	(расшифровка подписи)

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Минзов А.С. Идентификатор: R17801759-MinzovAS-e8de8907	А.С. Минзов
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)

Заведующий выпускающей кафедры	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Невский А.Ю. Идентификатор: R4bc65573-NevskyAY-0b6e493d	А.Ю. Невский
(должность, ученая степень, ученое звание)	(подпись)	(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

1 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$_{ПК-1}$ Проводит контрольные проверки работоспособности и эффективности применяемых программно-аппаратных средств защиты информации	Знать: основы методологии «Общих критериев» для практического использования при оценке безопасности информационных технологий 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 Уметь: применять современное и эффективное средство управления безопасностью информационных технологий на основе	Тест 1. Зарубежный опыт разработки критериев оценки безопасности информационных технологий (Тестирование) Контрольная работа 1. Практическое применение «Общих критериев» оценки безопасности информационных технологий для разработки профилей защиты и заданий по безопасности (Контрольная работа) Тест 2. Терминология и общая модель критериев оценки безопасности информационных технологий (ГОСТ Р ИСО/МЭК 15408). Защита результатов, полученных на практическом занятии №7 (Тестирование)

		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$_{ПК-2}$ Тестирует системы защиты информации автоматизированных систем	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:

Знать: основы методологии «Общих критериев» для практического использования при оценке безопасности информационных технологий	1.Как называется вторая часть ОК? 1. Компоненты доверия к безопасности 2. Функциональные компоненты безопасности 3. Руководство по разработке заданий по безопасности 4. Руководство по разработке профилей защиты 2.Международная организация по стандартизации имеет аббревиатуру 1. ISO 2. IEC 3. ИСО 4. 3 5. 1 и 3 3.Стандартизацией в какой области не занимается ISO? 1. занимается всеми 2. электротехника и электроника 3. криптография 4. техническая защита информации
Уметь: применять современное и эффективное средство управления безопасностью информационных технологий на основе использования отечественных и международных стандартов	1.Какие документы разработаны ISO для поддержки ОК? 1. Руководство по разработке ПЗ и ЗБ 2. Процедуры регистрации ПЗ 3. 1 и 2 4. Общая методология оценки безопасности ИТ 5. 1 и 4 6. 1,2,4 2.Какой разрешенной операции на компонентах нет в ОК? 1. Итерация 2. Повторение 3. Уточнение 4. Выбор 5. Назначение

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:

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.Стандартизацией в какой области занимается международная организация IEC? 1. Электротехники и электроники 2. Электротехники, электроники и радиосвязи 3. Приборостроения 4. Смежных технологий 5. 1-3 6. Все перечисленные 2.Для каких структурных частей требований доверия предполагается описание ЦЕЛИ? 1. Класс 2. Семейство 3. Компонент 4. Элемент 5. Класс и семейство 6. Семейство и компонент 3.Какой уровень доверия предполагает полуформальную верификацию проекта и тестирование? 1. 2 2. 4 3. 6 4. 8
Уметь: проводить обоснование перечня функциональных компонент безопасности при разработке профилей защиты и заданий по безопасности	1.Какое положение не относится к ограничениям на применение ОК? 1. нет критериев для административных мер; 2. не рассматривается административно-правовая структура;

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

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:

Знать: порядок, технологию и критерии оценки (оценочные уровни доверия) к безопасности информационных технологий и их сущность	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»?
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.)	1.Какой вид зависимости в таблицах зависимостей для функциональных компонентов обозначается символом «X»? 2.Каковы задачи оценки, сформулирован в ОМО? Их общая характеристика

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

1 семестр

Форма промежуточной аттестации: Экзамен

Пример билета

НИУ МЭИ	**ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1** Кафедра *Безопасности и информационных технологий* Дисциплина «**КРИТЕРИИ ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ**»	*Утверждаю:* *Зав. каф. БИТ* *А.Ю.Невский* 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

I. Перечень компетенций/индикаторов и контрольных вопросов проверки результатов освоения дисциплины

1. Компетенция/Индикатор: ПК-1.1$_{ПК-1}$ 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$_{ПК-2}$ 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.