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

Рабочая программа дисциплины
КРИТЕРИИ ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Блок:	**Блок 1 «Дисциплины (модули)»**
Часть образовательной программы:	**Вариативная**
№ дисциплины по учебному плану:	**Б1.В.01**
Трудоемкость в зачетных единицах:	**1 семестр - 5;**
Часов (всего) по учебному плану:	**180 часов**
Лекции	**1 семестр - 16 часов;**
Практические занятия	**1 семестр - 48 часа;**
Лабораторные работы	**не предусмотрено учебным планом**
Консультации	**проводится в рамках часов аудиторных занятий**
Самостоятельная работа	**1 семестр - 115,7 часов;**
в том числе на КП/КР	**не предусмотрено учебным планом**
Иная контактная работа	**проводится в рамках часов аудиторных занятий**
включая: **Тестирование** **Проверочная работа**	
Промежуточная аттестация:	
Зачет с оценкой	**1 семестр - 0,3 часа;**

Москва 2020

ПРОГРАММУ СОСТАВИЛ:

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)

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель освоения дисциплины: является формирование у обучаемых знаний и умений практического использования приемов и способов разработки профилей защиты и заданий по безопасности для оценки эффективности и степени доверия к безопасности образцов наиболее распространенных информационных технологий на основе использования методологического подхода «Общих критериев оценки безопасности информационных технологий» (серия стандартов ГОСТ Р ИСО/МЭК 15408) и методических документов, сопровождающих эти стандарты

Задачи дисциплины

- формирование знаний по «методологии», структуре, общему содержанию серии стандартов ГОСТ Р ИСО/МЭК 15408, а также методике их применения для оценки безопасности информационных технологий;;
- обучение разработке профилей защиты и заданий по безопасности для оценки эффективности и степени доверия к безопасности информационных технологий;;
- овладение обучаемыми современным и эффективным средством управления безопасностью информационных технологий..

Формируемые у обучающегося **компетенции** и запланированные **результаты обучения** по дисциплине, соотнесенные с **индикаторами достижения компетенций**:

Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**	**Запланированные результаты обучения**
ПК-1 способностью анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты		знать: - основы методологии «Общих критериев» для практического использования при оценке безопасности информационных технологий;. уметь: - применять современное и эффективное средство управления безопасностью информационных технологий на основе использования отечественных и международных стандартов;.
ПК-3 способностью проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов		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;. уметь: - проводить обоснование перечня функциональных компонент безопасности при разработке профилей защиты и заданий по безопасности информационных технологий;.
ПК-14 способностью		знать:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Запланированные результаты обучения
организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документамиФСБ России, ФСТЭК России		- 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.).;.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к части, формируемой участниками образовательных отношений блока дисциплин основной профессиональной образовательной программе Управление информационной безопасностью (далее – ОПОП), направления подготовки 10.04.01 Информационная безопасность, уровень образования: высшее образование - магистратура.

Базируется на уровне среднего общего образования.

Результаты обучения, полученные при освоении дисциплины, необходимы при выполнении выпускной квалификационной работы.

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 5 зачетных единиц, 180 часов.

№ п/п	Разделы/темы дисциплины/формы промежуточной аттестации	Всего часов на раздел	Семестр	Распределение трудоемкости раздела (в часах) по видам учебной работы										Содержание самостоятельной работы/ методические указания
				Контактная работа								СР		
				Лек	Лаб	Пр	Консультация		ИКР		ПА	Работа в семестре	Подготовка к аттестации /контроль	
							КПР	ГК	ИККП	ТК				
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	Основные требования безопасности информационных технологий	40	1	4	-	12	-	-	-	-	-	24	-	***Самостоятельное изучение теоретического материала:*** Канадские критерии оценки доверенных информационных технологий, CTCSEC
1.1	Подходы к разработке критериев оценки безопасности информационных технологий. (Зарубежный опыт).	20		2	-	6	-	-	-	-	-	12	-	***Самостоятельное изучение теоретического материала:*** Изучение истории возникновения и развития критериев оценки безопасности информационных технологий на примере положений "Оранжевой книги" США, TCSEC ***Изучение материалов литературных источников:*** [3], 1-111 [4], 1-98 [5], 45-56
1.2	Разработка единых критериев оценки безопасности информационных технологий	20		2	-	6	-	-	-	-	-	12	-	
2	Стандарты серии ГОСТ Р ИСО/МЭК 15408 «Общие критерии». Систематизированные каталоги функциональных компонент безопасности и доверия к безопасности информационных	66		8	-	22	-	-	-	-	-	36	-	***Подготовка домашнего задания:*** Для выбранного САВЗ выбрать стандартные компоненты доверия к безопасности из каталога, содержащегося в ГОСТ Р ИСО/МЭК 15408. Часть 3. Сформировать вывод о достаточности стандартных компонент доверия безопасности для описания данного продукта ИТ. ***Подготовка домашнего задания:*** На основе разработанного перечня функций безопасности для САВЗ выбрать стандартные компоненты безопасности из

	технологий.													каталога, содержащегося в ГОСТ Р
2.1	Общая модель критериев оценки безопасности информационных технологий.	20		2	-	6	-	-	-	-	-	12	-	ИСО/МЭК 15408. Часть 2. Сформировать вывод о достаточности стандартных компонент безопасности для описания данного продукта ИТ. ***Подготовка домашнего задания:*** Разработка студентами перечня функций безопасности для средства антивирусной защиты информации (САВЗ) ***Изучение материалов литературных источников:*** [1], 1-88
2.2	Критерии оценки безопасности информационных технологий. Функциональные компоненты безопасности	23		3	-	8	-	-	-	-	-	12	-	
2.3	Критерии оценки безопасности информационных технологий. Компоненты доверия к безопасности.	23		3	-	8	-	-	-	-	-	12	-	
3	Практическое применение подходов «Общих» критериев при разработке задания по безопасности для конкретного класса информационных технологий.	56		4	-	14	-	-	-	-	-	38	-	***Подготовка доклада, выступления:*** Выступить сообщением о разработанном задании по безопасности продукта ИТ-технологии из класса киберфизических систем, его содержании и сущности основных разделов ***Подготовка домашнего задания:*** В соответствии с индивидуальным заданием осуществить выбор продукта ИТ-технологии из класса киберфизических систем и для него разработать задание по безопасности ***Изучение материалов литературных источников:*** [2], 1-230
3.1	Практическое применение «Общих критериев» оценки безопасности информационных технологий.	36		2	-	10	-	-	-	-	-	24	-	
3.2	Методология оценки безопасности информационных технологий.	20		2	-	4	-	-	-	-	-	14	-	
	Зачет с оценкой	18.0		-	-	-	-	-	-	-	0.3	-	17.7	

	Всего за семестр	**180.0**		**16**	**-**	**48**	**-**	**-**	**-**	**-**	**0.3**	**98**	**17.7**	
	Итого за семестр	**180.0**		**16**	**-**	**48**	**-**		**-**		**0.3**	**115.7**		

Примечание: Лек – лекции; Лаб – лабораторные работы; Пр – практические занятия; КПР – аудиторные консультации по курсовым проектам/работам; ИККП – индивидуальные консультации по курсовым проектам/работам; ГК- групповые консультации по разделам дисциплины; СР – самостоятельная работа студента; ИКР – иная контактная работа; ТК – текущий контроль; ПА – промежуточная аттестация

3.2 Краткое содержание разделов

1. Основные требования безопасности информационных технологий

1.1. Подходы к разработке критериев оценки безопасности информационных технологий. (Зарубежный опыт).

Анализ опыта зарубежных государств у оценке безопасности информационных технологий.

1.2. Разработка единых критериев оценки безопасности информационных технологий

История разработки единых критериев оценки безопасности информационных технологий и современное их состояние.

2. Стандарты серии ГОСТ Р ИСО/МЭК 15408 «Общие критерии». Систематизированные каталоги функциональных компонент безопасности и доверия к безопасности информационных технологий.

2.1. Общая модель критериев оценки безопасности информационных технологий.

Содержание и сущность общей модели критериев оценки безопасности информационных технологий.

2.2. Критерии оценки безопасности информационных технологий. Функциональные компоненты безопасности

Перечень и общая характеристика стандартного набора функциональных компонентов безопасности.

2.3. Критерии оценки безопасности информационных технологий. Компоненты доверия к безопасности.

Перечень и общая характеристика стандартного набора компонентов доверия к безопасности..

3. Практическое применение подходов «Общих» критериев при разработке задания по безопасности для конкретного класса информационных технологий.

3.1. Практическое применение «Общих критериев» оценки безопасности информационных технологий.

Разработка основного содержания задания по безопасности для конкретного класса информационных технологий..

3.2. Методология оценки безопасности информационных технологий.

Изучение и практическое применение документов, сопровождающих "Общие критерии".

3.3. Темы практических занятий

1. Виды требований безопасности (функциональные компоненты и компоненты доверия);
2. Основные конструкции (информационные структуры) представления требований безопасности (профиль защиты, задание по безопасности).;
3. Основные методические положения по оценке безопасности продуктов ИТ.;
4. Универсальный систематизированный каталог функциональных компонент безопасности.;
5. Систематизированный каталог компонент доверия к безопасности и оценочные

уровни доверия.;
6. Практическое применение «Общих критериев» оценки безопасности информационных технологий для разработки профилей защиты и заданий по безопасности.;
7. Практическое применение положений методологии оценки безопасности информационных технологий..

3.4. Темы лабораторных работ

не предусмотрено

3.5 Консультации

Групповые консультации по разделам дисциплины (ГК)

1. Основное содержание и положения "Оранжевой книги" США о критериях оценки информационных систем (TCSEC).
2. История развития и современное состояние "Единых критериев оценки безопасности информационных технологий"
3. Общее содержание каталога компонент оценки безопасности информационных технологий. Иерархия каталога: класс-семейство-компонент-элемент безопасности. Структура каталога.
4. Общее содержание каталога компонент доверия к безопасности информационных технологий. Иерархия каталога: класс-семейство-компонент-элемент доверия к безопасности. Структура каталога.
5. Выполнение индивидуального задания "Разработка задания по безопасности для продукта информационных технологий из класса киберфизических систем.

Текущий контроль (ТК)

1. Основное содержание и положения канадских критериев оценки безопасности доверенных информационных систем (CTCSEC).

3.6 Тематика курсовых проектов/курсовых работ

Курсовой проект/ работа не предусмотрены

3.7. Соответствие разделов дисциплины и формируемых в них компетенций

Запланированные результаты обучения по дисциплине (в соответствии с разделом 1)	Коды индикаторов	Номер раздела дисциплины (в соответствии с п.3.1)			Оценочное средство (тип и наименование)
		1	2	3	
Знать:					
основы методологии «Общих критериев» для практического использования при оценке безопасности информационных технологий;	ПК-1(Компетенция)	+		+	Тестирование/Тест 1
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;	ПК-3(Компетенция)		+		Проверочная работа/Практическое задание
порядок, технологию и критерии оценки (оценочные уровни доверия) к безопасности информационных технологий и их сущность;	ПК-14(Компетенция)		+		Проверочная работа/Практическое задание
Уметь:					
применять современное и эффективное средство управления безопасностью информационных технологий на основе использования отечественных и международных стандартов;	ПК-1(Компетенция)			+	Проверочная работа/Практическое задание
проводить обоснование перечня функциональных компонент безопасности при разработке профилей защиты и заданий по безопасности информационных технологий;	ПК-3(Компетенция)			+	Проверочная работа/Практическое задание
выполнять в полном объеме разработку задания по безопасности для образца информационной технологии, включая нетривиальные реализации (киберфизические системы, облачные технологии, технологии больших данных и др.).;	ПК-14(Компетенция)			+	Тестирование/Тест 1

4. КОМПЕТЕНТНОСТНО-ОРИЕНТИРОВАННЫЕ ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ КОНТРОЛЯ ОСВОЕНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (ТЕКУЩИЙ КОНТРОЛЬ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ПО ДИСЦИПЛИНЕ)

4.1. Текущий контроль успеваемости

1 семестр

Форма реализации: Выполнение задания

1. Тест 1 (Тестирование)

Форма реализации: Письменная работа

1. Практическое задание (Проверочная работа)
2. Практическое задание (Проверочная работа)

Балльно-рейтинговая структура дисциплины является приложением А.

4.2 Промежуточная аттестация по дисциплине

Зачет с оценкой (Семестр №1)

Итоговая оценка выставляется в соответствии с системой БАРС, исходя из семестровой и зачетной составляющей

В диплом выставляется оценка за 1 семестр.

Примечание: Оценочные материалы по дисциплине приведены в фонде оценочных материалов ОПОП.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1 Печатные и электронные издания:

1. Хорев, П. Б. Защита информационных систем : учебное пособие по курсам "Защита информации", "Методы и средства защиты компьютерной информации" по направлениям "Прикладная математика и информатика", "Информационные системы и технологии" и "Прикладная информатика" / П. Б. Хорев, Моск. энерг. ин-т (МЭИ ТУ) . – М. : Издательский дом МЭИ, 2010 . – 88 с. - ISBN 978-5-383-00546-0 . http://elib.mpei.ru/action.php?kt_path_info=ktcore.SecViewPlugin.actions.document&fDocumentId=1956;
2. Зайцев, А. П. Технические средства и методы защиты информации : учебник для вузов по группе специальностей "Информационная безопасность" / А. П. Зайцев, Р. В. Мещеряков, А. А. Шелупанов . – 7-е изд . – М. : Горячая Линия-Телеком, 2012 . – 442 с. - ISBN 978-5-9912-0233-6 .;
3. Бабаш, А. В. Актуальные вопросы защиты информации : монография / А. В. Бабаш, Е. К. Баранова . – Москва : РИОР : ИНФРА-М, 2021 . – 111 с. – (Научная мысль) . - ISBN 978-5-369-01680-0 .;
4. Система менеджмента информационной безопасности ГОСТ Р ИСО/МЭК 27001-2006 (проекты документов) : [учебно-методическое пособие] / А. С. Минзов, А. Ю. Невский, О. Р. Баронов, Р. А. Сюбаев, М-во образования и науки Рос. Федерации, Нац. исслед. ун-т "МЭИ" (НИУ"МЭИ"), Инженерно-экономич. ин-т национального исслед. ун-та "МЭИ", Кафедра "Безопасности и Информационных Технологий" (БИТ) . – М. : ВНИИгеосистем, 2019 . – 98 с. - Авт. указаны на обороте тит. л. - ISBN 978-5-8481-0234-5 .;
5. А. А. Титов- "Инженерно-техническая защита информации", Издательство: "Томский государственный университет систем управления и радиоэлектроники", Томск, 2010 - (195

с.)
https://biblioclub.ru/index.php?page=book&id=208567.

5.2 Лицензионное и свободно распространяемое программное обеспечение:
1. СДО "Прометей";
2. Office / Российский пакет офисных программ;
3. Windows / Операционная система семейства Linux;
4. Майнд Видеоконференции.

5.3 Интернет-ресурсы, включая профессиональные базы данных и информационно-справочные системы:
1. **ЭБС Лань** - https://e.lanbook.com/
2. **ЭБС "Университетская библиотека онлайн"** - http://biblioclub.ru/index.php?page=main_ub_red
3. **Научная электронная библиотека** - https://elibrary.ru/
4. **База данных ВИНИТИ online** - http://www.viniti.ru/
5. **База данных журналов издательства Elsevier** - https://www.sciencedirect.com/
6. **Электронные ресурсы издательства Springer** - https://link.springer.com/
7. **База данных Web of Science** - http://webofscience.com/
8. **База данных Scopus** - http://www.scopus.com
9. **Национальная электронная библиотека** - https://rusneb.ru/
10. **ЭБС "Консультант студента"** - http://www.studentlibrary.ru/
11. **Журналы American Chemical Society** - https://www.acs.org/content/acs/en.html
12. **Журналы American Institute of Physics** - https://www.scitation.org/
13. **Журналы American Physical Society** - https://journals.aps.org/about
14. **База данных издательства Annual Reviews Science Collection** - https://www.annualreviews.org/

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Тип помещения	Номер аудитории, наименование	Оснащение
Учебные аудитории для проведения лекционных занятий и текущего контроля	К-307, Учебная лаборатория "Открытое программное обеспечение"	стол преподавателя, стол компьютерный, стол учебный, стул, вешалка для одежды, тумба, компьютерная сеть с выходом в Интернет, мультимедийный проектор, экран, доска маркерная, сервер, компьютер персональный, кондиционер
	К-601, Учебная аудитория	парта со скамьей, стол преподавателя, стул, трибуна, доска меловая, мультимедийный проектор, экран
Учебные аудитории для проведения практических занятий, КР и КП	К-307, Учебная лаборатория "Открытое программное обеспечение"	стол преподавателя, стол компьютерный, стол учебный, стул, вешалка для одежды, тумба, компьютерная сеть с выходом в Интернет, мультимедийный проектор, экран, доска маркерная, сервер, компьютер персональный, кондиционер
Учебные аудитории для проведения промежуточной аттестации	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
	А-300, Учебная аудитория "А"	кресло рабочее, парта, стеллаж, стол преподавателя, стол учебный, стул, трибуна, микрофон, мультимедийный

		проектор, экран, доска маркерная, колонки, техническая аппаратура, кондиционер, телевизор
Помещения для самостоятельной работы	НТБ-303, Компьютерный читальный зал	стол компьютерный, стул, стол письменный, вешалка для одежды, компьютерная сеть с выходом в Интернет, компьютер персональный, принтер, кондиционер
Помещения для консультирования	А-300, Учебная аудитория "А"	кресло рабочее, парта, стеллаж, стол преподавателя, стол учебный, стул, трибуна, микрофон, мультимедийный проектор, экран, доска маркерная, колонки, техническая аппаратура, кондиционер, телевизор
Помещения для хранения оборудования и учебного инвентаря	К-202/2, Склад кафедры БИТ	стеллаж для хранения инвентаря, стол, стул, шкаф для документов, шкаф для хранения инвентаря, тумба, запасные комплектующие для оборудования

Приложение А

БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА ДИСЦИПЛИНЫ

Критерии оценки безопасности информационных технологий

(название дисциплины)

1 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:
КМ-1 Тест 1 (Тестирование)
КМ-2 Практическое задание (Проверочная работа)
КМ-3 Практическое задание (Проверочная работа)

Вид промежуточной аттестации – Зачет с оценкой.

Номер раздела	Раздел дисциплины	Индекс КМ:	КМ-1	КМ-2	КМ-3
		Неделя КМ:	4	8	12
1	Основные требования безопасности информационных технологий				
1.1	Подходы к разработке критериев оценки безопасности информационных технологий. (Зарубежный опыт).		+		
1.2	Разработка единых критериев оценки безопасности информационных технологий		+		
2	Стандарты серии ГОСТ Р ИСО/МЭК 15408 «Общие критерии». Систематизированные каталоги функциональных компонент безопасности и доверия к безопасности информационных технологий.				
2.1	Общая модель критериев оценки безопасности информационных технологий.				+
2.2	Критерии оценки безопасности информационных технологий. Функциональные компоненты безопасности				+
2.3	Критерии оценки безопасности информационных технологий. Компоненты доверия к безопасности.			+	
3	Практическое применение подходов «Общих» критериев при разработке задания по безопасности для конкретного класса информационных технологий.				
3.1	Практическое применение «Общих критериев» оценки безопасности информационных технологий.		+	+	+
3.2	Методология оценки безопасности информационных технологий.		+		
		Вес КМ, %:	30	30	40