

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

---

Направление подготовки/специальность: 10.03.01 Информационная безопасность

Наименование образовательной программы: Безопасность автоматизированных систем

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очная

**Рабочая программа дисциплины**  
**РОССИЙСКИЕ И МЕЖДУНАРОДНЫЕ СТАНДАРТЫ**  
**ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

<b>Блок:</b>	Блок 1 «Дисциплины (модули)»
<b>Часть образовательной программы:</b>	Часть, формируемая участниками образовательных отношений
<b>№ дисциплины по учебному плану:</b>	Б1.Ч.08
<b>Трудоемкость в зачетных единицах:</b>	8 семестр - 4;
<b>Часов (всего) по учебному плану:</b>	144 часа
<b>Лекции</b>	8 семестр - 28 часа;
<b>Практические занятия</b>	8 семестр - 56 часа;
<b>Лабораторные работы</b>	не предусмотрено учебным планом
<b>Консультации</b>	8 семестр - 2 часа;
<b>Самостоятельная работа</b>	8 семестр - 57,5 часа;
<b>в том числе на КП/КР</b>	не предусмотрено учебным планом
<b>Иная контактная работа</b>	проводится в рамках часов аудиторных занятий
<b>включая:</b>	
<b>Контрольная работа</b>	
<b>Промежуточная аттестация:</b>	
<b>Экзамен</b>	8 семестр - 0,50 часа;

Москва 2022

## ПРОГРАММУ СОСТАВИЛ:

Преподаватель

(должность)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Унижаев Н.В.
	Идентификатор	Rb43f42d6-UnizhayevNV-2454ef2f

(подпись)


Н.В. Унижаев

(расшифровка  
подписи)

## СОГЛАСОВАНО:

Руководитель  
образовательной программы

(должность, ученая степень, ученое звание)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Баронов О.Р.
	Идентификатор	R90d76356-BaronovOR-7bf8fd7e

(подпись)

О.Р. Баронов

(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)

## 1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

**Цель освоения дисциплины:** Изучение основ международного и национального регулирования стандартизации в области информационной безопасности, содержания наиболее значимых национальных и международных стандартов в области информационной безопасности, а также формирование умения применять знания положений и требований стандартов для разработки нормативных документов организации

### Задачи дисциплины

- изучение основ международного и национального регулирования стандартизации в области информационной безопасности;;
- изучение основного содержания наиболее значимых стандартов (серий стандартов) в области безопасности информационных технологий;;
- приобретение умения применять знание положений стандартов для разработки нормативных документов организации в области информационной безопасности;;
- формирование готовности и способности использовать положения стандартов в практической деятельности..

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-2 Готов к внедрению систем защиты информации автоматизированных систем	ПК-2.2 <sub>ПК-2</sub> Разрабатывает организационно-распорядительные документы по защите информации в автоматизированных системах	знать: - – требования к организационным мерам по защите информации в автоматизированных системах;; - – ограничения к организационным мерам по защите информации в автоматизированных системах;.  уметь: - – требования к организационным мерам по защите информации в автоматизированных системах;; - – ограничения к организационным мерам по защите информации в автоматизированных системах;.
ПК-2 Готов к внедрению систем защиты информации автоматизированных систем	ПК-2.3 <sub>ПК-2</sub> Внедряет организационные меры по защите информации в автоматизированных системах	знать: - – нормативные правовые документы по информационной безопасности;; - – общие сведения о международных и национальных организациях, выполняющих полномочия в области стандартизации, характере их деятельности, а также современных редакций национальных и международных стандартов в области менеджмента информационной безопасности;.  уметь: - – практически разрабатывать критерии оценки безопасности информационных

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Запланированные результаты обучения
		технологий на основе требований международных стандартов; - – применять требования действующих стандартов по информационной безопасности;

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к основной профессиональной образовательной программе Безопасность автоматизированных систем (далее – ОПОП), направления подготовки 10.03.01 Информационная безопасность, уровень образования: высшее образование - бакалавриат.

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 4 зачетных единицы, 144 часа.

№ 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	Зарубежные и международные стандарты в области информационной безопасности и их анализ	32	8	8	-	16	-	-	-	-	-	8	-	<p><b><u>Подготовка к текущему контролю:</u></b> Повторение материала по разделу "Зарубежные и международные стандарты в области информационной безопасности и их анализ"</p> <p><b><u>Подготовка к лабораторной работе:</u></b> Для выполнения заданий по лабораторной работе необходимо предварительно изучить тему и задачи выполнения лабораторной работы, а так же изучить вопросы вариантов обработки результатов по изученному в разделе "Зарубежные и международные стандарты в области информационной безопасности и их анализ" материалу.</p> <p><b><u>Подготовка к аудиторным занятиям:</u></b> Проработка лекции, выполнение и подготовка к защите лаб. работы</p> <p><b><u>Подготовка домашнего задания:</u></b> Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Зарубежные и международные стандарты в области информационной безопасности и их анализ" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по</p>
1.1	Вводная лекция	8		2	-	4	-	-	-	-	-	2	-	
1.2	Тема 1.	8		2	-	4	-	-	-	-	-	2	-	
1.3	Тема 2.	8		2	-	4	-	-	-	-	-	2	-	
1.4	Тема 3.	8		2	-	4	-	-	-	-	-	2	-	

														представленным письменным работам. <b><u>Подготовка к контрольной работе:</u></b> Изучение материалов по разделу Зарубежные и международные стандарты в области информационной безопасности и их анализ и подготовка к контрольной работе <b><u>Подготовка к практическим занятиям:</u></b> Подготовка практического задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Зарубежные и международные стандарты в области информационной безопасности и их анализ" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам. <b><u>Самостоятельное изучение теоретического материала:</u></b> Изучение дополнительного материала по разделу "Зарубежные и международные стандарты в области информационной безопасности и их анализ" <b><u>Изучение материалов литературных источников:</u></b> [1], 16-37 [3], 46-58 [4], 27-89 [6], 11-46 [8], 15-77 [11], 48-184
2	Национальные стандарты РФ в области информационной безопасности и их анализ	32	8	-	16	-	-	-	-	-	8	-	<b><u>Подготовка к текущему контролю:</u></b> Повторение материала по разделу "Национальные стандарты РФ в области информационной безопасности и их анализ" <b><u>Проведение исследований:</u></b> Работа выполняется по индивидуальному заданию. Для проведения исследования применяется	
2.1	Тема 4.	8	2	-	4	-	-	-	-	-	2	-		

2.2	Тема 5.	8		2	-	4	-	-	-	-	-	2	-	<p>материалы представление преподавателем</p> <p><b><u>Подготовка расчетно-графического задания:</u></b> В рамках расчетно-графического задания выполняется чертеж конструкции. Для выполнения чертежей выполняются предварительные расчеты основных показателей, которые указываются на чертеже. Задание выполняется индивидуально по вариантам.</p> <p><b><u>Подготовка курсового проекта:</u></b> Курсовой проект выполняется по индивидуальному заданию. В рамках работы необходимо рассчитать основные показатели работы оборудования, выбрать оптимальное решение. Курсовой проект предусматривает пояснительную записку с расчетами и графическую часть.</p> <p><b><u>Подготовка к лабораторной работе:</u></b> Для выполнения заданий по лабораторной работе необходимо предварительно изучить тему и задачи выполнения лабораторной работы, а так же изучить вопросы вариантов обработки результатов по изученному в разделе "Национальные стандарты РФ в области информационной безопасности и их анализ" материалу.</p> <p><b><u>Подготовка к аудиторным занятиям:</u></b> Проработка лекции, выполнение и подготовка к защите лаб. работы</p> <p><b><u>Подготовка домашнего задания:</u></b> Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Национальные стандарты РФ в области информационной безопасности и их анализ" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по</p>
2.3	Тема 6.	8		2	-	4	-	-	-	-	-	2	-	
2.4	Тема 7.	8		2	-	4	-	-	-	-	-	2	-	

															<p>представленным письменным работам.</p> <p><b><u>Подготовка доклада, выступления:</u></b>  Задание связано с углубленным изучением разделов дисциплины и самостоятельным поиском материалов для раскрытия темы доклада. Материалы выполненной работы представляются в электронном виде или в форме распечатанных презентационных слайдов.</p> <p><b><u>Подготовка к контрольной работе:</u></b>  Изучение материалов по разделу Национальные стандарты РФ в области информационной безопасности и их анализ и подготовка к контрольной работе</p> <p><b><u>Подготовка курсовой работы:</u></b> Курсовая работа представлена в виде крупной задачи по учебному кейсу, охватывающей несколько расчетных вопросов и выбор варианта проектного решения. Пример задания:</p> <p><b><u>Подготовка к практическим занятиям:</u></b>  Изучение материала по разделу "Национальные стандарты РФ в области информационной безопасности и их анализ" подготовка к выполнению заданий на практических занятиях</p> <p><b><u>Самостоятельное изучение теоретического материала:</u></b> Изучение дополнительного материала по разделу "Национальные стандарты РФ в области информационной безопасности и их анализ"</p> <p><b><u>Изучение материалов литературных источников:</u></b></p> <p>[2], 44-86  [4], 39-55  [5], 65-68  [7], 39-46  [10], 58-87  [11], 69-111</p>
--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	---



3	Практика применения «Общих критериев» для разработки профилей защиты и заданий по безопасности информационных технологий	44		12	-	24	-	-	-	-	-	8	-	<p><b><u>Подготовка к текущему контролю:</u></b> Повторение материала по разделу "Практика применения «Общих критериев» для разработки профилей защиты и заданий по безопасности информационных технологий"</p> <p><b><u>Подготовка к лабораторной работе:</u></b> Для выполнения заданий по лабораторной работе необходимо предварительно изучить тему и задачи выполнения лабораторной работы, а так же изучить вопросы вариантов обработки результатов по изученному в разделе "Практика применения «Общих критериев» для разработки профилей защиты и заданий по безопасности информационных технологий" материалу.</p> <p><b><u>Подготовка к аудиторным занятиям:</u></b> Проработка лекции, выполнение и подготовка к защите практических работы</p> <p><b><u>Подготовка домашнего задания:</u></b> Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Практика применения «Общих критериев» для разработки профилей защиты и заданий по безопасности информационных технологий" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам.</p> <p><b><u>Подготовка доклада, выступления:</u></b> Задание связано с углубленным изучением разделов дисциплины и самостоятельным поиском материалов для раскрытия темы доклада. Материалы выполненной работы представляются в электронном виде или в форме распечатанных презентационных слайдов. В качестве тем докладов студентам</p>
3.1	Тема 8.	10		2	-	6	-	-	-	-	-	2	-	
3.2	Тема 9.	12		4	-	6	-	-	-	-	-	2	-	
3.3	Тема 10.	10		2	-	6	-	-	-	-	-	2	-	
3.4	Тема 11.	12		4	-	6	-	-	-	-	-	2	-	

												<p>предлагаются варианты представленные преподавателем</p> <p><b><u>Подготовка к контрольной работе:</u></b> Изучение материалов по разделу Практика применения «Общих критериев» для разработки профилей защиты и заданий по безопасности информационных технологий и подготовка к контрольной работе по различным темам</p> <p><b><u>Подготовка к практическим занятиям:</u></b> Изучение материала по разделу "Практика применения «Общих критериев» для разработки профилей защиты и заданий по безопасности информационных технологий" подготовка к выполнению заданий на практических занятиях</p> <p><b><u>Самостоятельное изучение теоретического материала:</u></b> Изучение дополнительного материала по разделу "Практика применения «Общих критериев» для разработки профилей защиты и заданий по безопасности информационных технологий"</p> <p><b><u>Подготовка расчетных заданий:</u></b> Задания ориентированы на решения минизадач по разделу "Практика применения «Общих критериев» для разработки профилей защиты и заданий по безопасности информационных технологий". Студенты необходимо повторить теоретический материал, разобрать примеры решения аналогичных задач. провести расчеты по варианту задания и сделать выводы. В качестве задания используются следующие упражнения:</p> <p><b><u>Изучение материалов литературных источников:</u></b></p> <p>[4], 112-144 [5], 55-98 [8], 37-58</p>
--	--	--	--	--	--	--	--	--	--	--	--	--

														[9], 22-89 [11], 43-65
	Экзамен	36.00	-	-	-	-	2	-	-	0.50	-	33.50		
	Всего за семестр	144.00	28	-	56	-	2	-	-	0.50	24	33.50		
	Итого за семестр	144.00	28	-	56		2		-	0.50		57.50		

**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. Зарубежные и международные стандарты в области информационной безопасности и их анализ

##### 1.1. Вводная лекция

Краткие сведения об истории появления стандартов в области информационной безопасности. Последовательность развития стандартизации в области информационной безопасности. Международные организации, участвующие в разработке стандартов в области ИБ. Проблема гармонизации отечественных и зарубежных стандартов. Международные стандарты в области информационной безопасности..

##### 1.2. Тема 1.

Практические рекомендации британского института стандартов BSI по управлению информационной безопасностью. Британский национальный стандарт BS 7799: назначение, структура, последовательность развития, основное содержание. Анализ преимуществ и недостатков BS 7799. BS 7799 – основа разработки системы международных стандартов серии 27000 по менеджменту информационной безопасности. Анализ комплекса стандартов 27000 и последовательность их развития, структура и основное содержание. Принятие стандарта в качестве национального стандарта РФ.

##### 1.3. Тема 2.

Критерий оценки безопасности компьютерных систем США «Оранжевая книга». Основные положения: понятие надежной системы, критерии надежности, уровни надежности. Общая характеристика «цветных» документов США для оценки безопасности компьютерных систем. Деятельность национального института стандартов и технологий США NIST по стандартизации управления информационными рисками. Национальный стандарт США NIST 800-30..

##### 1.4. Тема 3.

Стандарт ФРГ BSI: «Руководство по базовому уровню защищенности информационных технологий». Порядок использования руководства при управлении информационной безопасностью, описание компонентов информационных технологий, каталоги угроз безопасности и контрмер. Порядок и последовательность анализа компонентов информационных технологий. Анализ преимуществ и недостатков BSI..

#### 2. Национальные стандарты РФ в области информационной безопасности и их анализ

##### 2.1. Тема 4.

Требования ФЗ-184 от 27.12.2002 г. «О техническом регулировании». Цели и принципы стандартизации в РФ. Национальные органы стандартизации РФ и анализ их полномочий. Требования ГОСТ Р 1.0 – 2004 Стандартизация в РФ. Основные положения. Особенности развития отечественных нормативных документов в области информационной безопасности. Типы документов стандартизации, разрабатываемые в национальной системе стандартов..

##### 2.2. Тема 5.

Стандартизация в области информационной безопасности РФ. Классификация и структура стандартов. Требования ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Стандартизация основных терминов и определений в области ИБ..

### 2.3. Тема 6.

Стандартизация РФ в области криптографической защиты информации. Стандартизация алгоритмов криптографического преобразования информации. Положения стандарта ГОСТ 28147-89. Стандартизация процессов формирования и проверки электронной цифровой подписи. Положения стандарта ГОСТ Р 34.10-2012. Стандартизация криптографической защиты информации с использованием функций хэширования. Положения стандарта ГОСТ Р 34.11-2012.

### 2.4. Тема 7.

Проблема оценки уровня безопасности информационных технологий. История создания и разработки, общая парадигма «Общих критериев». Структура международных стандартов серии 15408: наименование, назначение, структура, основное содержание частей стандарта. Практическое применение положений и требований стандарта..

## 3. Практика применения «Общих критериев» для разработки профилей защиты и заданий по безопасности информационных технологий

### 3.1. Тема 8.

ГОСТ Р ИСО/МЭК 15408-1-2012 Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Описание общей модели. Доработка требований безопасности «ОК» до конкретного применения. Понятие профиля защиты. Результаты оценки и практика их использования для оценки безопасности информационных технологий..

### 3.2. Тема 9.

ГОСТ Р ИСО/МЭК 15408-2-2013 Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности. Парадигма функциональных требований безопасности. Структура и иерархия класса компонентов. Перечень и каталог компонентов безопасности..

### 3.3. Тема 10.

ГОСТ Р ИСО/МЭК 15408-3-2013 Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности. Парадигма доверия к безопасности и шкала оценки доверия. Структура и иерархия классов доверия к безопасности. Понятие и детализация оценочных уровней доверия..

### 3.4. Тема 11.

Принятие стандартов серии 15408 в качестве руководящих документов ФСТЭК РФ по оценке безопасности информационных технологий. Практика применения требований «ОК». ГОСТ Р ИСО/МЭК 15446-2008 Руководство по разработке профилей защиты и заданий по безопасности. Краткий обзор содержания профилей защиты и заданий по безопасности объектов оценки..

## **3.3. Темы практических занятий**

1. Стандартизация РФ в области криптографической защиты информации.;
2. Стандартизация в области информационной безопасности РФ. Классификация и структура стандартов. Требования ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Стандартизация основных терминов и определений в области ИБ.;
3. ГОСТ Р ИСО/МЭК 15408-1-2012 Критерии оценки безопасности информационных

технологий. Часть 1. Введение и общая модель. Описание общей модели. Доработка требований безопасности «ОК» до конкретного применения. Понятие профиля защиты и задания по безопасности. ГОСТ Р ИСО/МЭК 15408-2-2013 Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности. Парадигма функциональных требований безопасности. Структура и иерархия класса компонентов. Перечень и каталог компонентов безопасности.;

4. Требования стандарта ГОСТ 28147-89. Стандартизация процессов формирования и проверки электронной цифровой подписи. Положения стандарта ГОСТ Р 34.10-2012. Стандартизация криптографической защиты информации с использованием функций хэширования. Положения стандарта ГОСТ Р 34.11-2012. История создания и разработки, общая парадигма «Общих критериев». Структура международных стандартов серии 15408: наименование, назначение, структура, основное содержание частей стандарта. Практическое применение положений и требований стандарта.;

5. Анализ комплекса стандартов 27000 и последовательность их развития, структура и основное содержание. Принятие стандартов серии 27000 в качестве национальных стандартов РФ. Практика применения требований стандарта ГОСТ Р ИСО/МЭК - 27002 – 2012 «Свод норм и правил менеджмента информационной безопасности» для разработки политики информационной безопасности организации.;

6. История стандартизации в области информационной безопасности. Последовательность развития стандартов в области информационной безопасности. Международные организации, разрабатывающие стандарты: Международная электротехническая комиссия, Международная организация по стандартизации, национальные организации по стандартизации.;

7. Проблема гармонизации отечественных и зарубежных стандартов. История, необходимость, анализ положительных и негативных проявлений гармонизации. Международные стандарты в области информационной безопасности.;

8. Практические рекомендации британского института стандартов BSI по управлению информационной безопасностью. Британский национальный стандарт BS 7799: назначение, структура, последовательность развития, основное содержание. Анализ преимуществ и недостатков BS 7799. BS 7799 – основа разработки системы международных стандартов серии 27000 по менеджменту информационной безопасности.;

9. Стандарт ФРГ BSI: «Руководство по базовому уровню защищенности информационных технологий». Порядок использования руководства при управлении информационной безопасностью, описание компонентов информационных технологий, каталоги угроз безопасности и контрмер. Порядок и последовательность анализа компонентов информационных технологий. Анализ преимуществ и недостатков BSI.;

10. Национальные органы стандартизации РФ и анализ их полномочий. Требования ГОСТ Р 1.0 – 2004 Стандартизация в РФ. Основные положения. Классификация и структура стандартов.;

11. Критерий оценки безопасности компьютерных систем США «Оранжевая книга». Основные положения: понятие надежной системы, критерии надежности, уровни надежности. Национальный стандарт США NIST 800-30..

#### **3.4. Темы лабораторных работ** не предусмотрено

#### **3.5 Консультации**

*Аудиторные консультации по курсовому проекту/работе (КПР)*

1. Консультации направлены на выполнение разделов курсового проекта под руководством наставника (преподавателя). В рамках часов на групповые консультации разбираются наиболее важные части расчетных заданий раздела "Зарубежные и международные стандарты в области информационной безопасности и их анализ"
2. Консультации направлены на выполнение разделов курсового проекта под руководством наставника (преподавателя). В рамках часов на групповые консультации разбираются наиболее важные части расчетных заданий раздела "Национальные стандарты РФ в области информационной безопасности и их анализ"
3. Консультации направлены на выполнение разделов курсового проекта под руководством наставника (преподавателя). В рамках часов на групповые консультации разбираются наиболее важные части расчетных заданий раздела "Практика применения «Общих критериев» для разработки профилей защиты и заданий по безопасности информационных технологий"

*Групповые консультации по разделам дисциплины (ГК)*

1. Обсуждение материалов по кейсам раздела "Зарубежные и международные стандарты в области информационной безопасности и их анализ"
2. Обсуждение материалов по кейсам раздела "Национальные стандарты РФ в области информационной безопасности и их анализ"
3. Обсуждение материалов по кейсам раздела "Практика применения «Общих критериев» для разработки профилей защиты и заданий по безопасности информационных технологий"

*Текущий контроль (ТК)*

1. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Практика применения «Общих критериев» для разработки профилей защиты и заданий по безопасности информационных технологий"

### **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	
<b>Знать:</b>					
– ограничения к организационным мерам по защите информации в автоматизированных системах;	ПК-2.2 <sub>ПК-2</sub>	+	+		Контрольная работа/КМ-1
– требования к организационным мерам по защите информации в автоматизированных системах;	ПК-2.2 <sub>ПК-2</sub>	+	+		Контрольная работа/КМ-2
– общие сведения о международных и национальных организациях, выполняющих полномочия в области стандартизации, характере их деятельности, а также современных редакций национальных и международных стандартов в области менеджмента информационной безопасности;	ПК-2.3 <sub>ПК-2</sub>		+	+	Контрольная работа/КМ-4
– нормативные правовые документы по информационной безопасности;	ПК-2.3 <sub>ПК-2</sub>	+	+	+	Контрольная работа/КМ-3
<b>Уметь:</b>					
– ограничения к организационным мерам по защите информации в автоматизированных системах;	ПК-2.2 <sub>ПК-2</sub>		+	+	Контрольная работа/КМ-1
– требования к организационным мерам по защите информации в автоматизированных системах;	ПК-2.2 <sub>ПК-2</sub>			+	Контрольная работа/КМ-2
– применять требования действующих стандартов по информационной безопасности;	ПК-2.3 <sub>ПК-2</sub>			+	Контрольная работа/КМ-3
– практически разрабатывать критерии оценки безопасности информационных технологий на основе требований международных стандартов;	ПК-2.3 <sub>ПК-2</sub>			+	Контрольная работа/КМ-4



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

### **4.1. Текущий контроль успеваемости**

**8 семестр**

Форма реализации: Компьютерное задание

1. КМ-1 (Контрольная работа)
2. КМ-3 (Контрольная работа)

Форма реализации: Проверка задания

1. КМ-2 (Контрольная работа)
2. КМ-4 (Контрольная работа)

Балльно-рейтинговая структура дисциплины является приложением А.

### **4.2 Промежуточная аттестация по дисциплине**

*Экзамен (Семестр №8)*

Экзамен. Оценка определяется в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ» на основании семестровой и экзаменационной составляющих. В приложение к диплому выносятся оценка за 8 семестр.

В диплом выставляется оценка за 8 семестр.

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

## **5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ**

### **5.1 Печатные и электронные издания:**

1. Capture the Flag [CTF]. Игровые модели подготовки специалистов в сфере компьютерной безопасности : [учебно-методическое пособие для преподавателей] / А. Ю. Егоров, А. С. Минзов, А. Ю. Невский, О. Р. Баронов, Инженерно-экономич. ин-т национального исслед. ун-та "МЭИ", Кафедра "Безопасности и Информационных Технологий" (БИТ) . – М. : ВНИИгеосистем, 2018 . – 72 с. - ISBN 978-5-8481-0232-1 .;
2. Минзов, А. С. Методология применения терминов и определений в сфере информационной, экономической и комплексной безопасности бизнеса : учебно-методическое пособие / А. С. Минзов, Л. М. Кунбутаев, Нац. исслед. ун-т "МЭИ", Ин-т безопасности бизнеса МЭИ (ТУ) . – М. : ВНИИгеосистем, 2011 . – 84 с. - ISBN 978-5-8481-0083-9 .;
3. "Информационные технологии: учебно-методический комплекс по специальности 052700 (071201) – «Библиотечно-информационная деятельность»" 5, Издательство: "Кемеровский государственный университет культуры и искусств (КемГУКИ)", Кемерово, 2012 - (31 с.) <https://biblioclub.ru/index.php?page=book&id=274197>;
4. "05.25.03 - Библиотекоеведение, библиографоведение и книговедение: сборник программ основной профессиональной образовательной программы послевузовского профессионального образования (аспирантура)", Издательство: "Кемеровский государственный университет культуры и искусств (КемГУКИ)", Кемерово, 2012 - (286 с.) <https://biblioclub.ru/index.php?page=book&id=273808>;

5. "Business Excellence", Издательство: "РИА «Стандарты и качество»", Москва, 2013 - (108 с.)  
<https://biblioclub.ru/index.php?page=book&id=215818;>
6. Агуреев, И. А. Инженерно-техническая защита информации. Ч. 3 : учебное пособие и лабораторный практикум для Инженерно-экономического института / И. А. Агуреев, А. Ю. Невский, С. С. Рыжиков, Инженерно-экономич. ин-т национального исслед. ун-та "МЭИ" . – Москва : ВНИИгеосистем, 2021 . – 98 с. - ISBN 978-5-8481-0250-5 .;
7. Минзов, А. С. Управление рисками информационной безопасности : [монография] / А. С. Минзов, А. Ю. Невский, О. Р. Баронов ; ред. А. С. Минзов ; Нац. исслед. ун-т "МЭИ" (НИУ"МЭИ"), Инженерно-экономич. ин-т национального исслед. ун-та "МЭИ", Кафедра "Безопасности и Информационных Технологий" (БИТ) . – Москва : ВНИИгеосистем, 2019 . – 106 с. - ISBN 978-5-8481-0240-6 .;
8. В. Д. Астафеев- "Управление качеством на основе использования международных стандартов ИСО серии 9000 и отечественных стандартов – ГОСТов", Издательство: "Лаборатория книги", Москва, 2012 - (109 с.)  
<https://biblioclub.ru/index.php?page=book&id=142539;>
9. "Business Excellence", Издательство: "РИА «Стандарты и качество»", Москва, 2015 - (108 с.)  
<https://biblioclub.ru/index.php?page=book&id=429036;>
10. А. В. Артемов- "Информационная безопасность: курс лекций", Издательство: "Межрегиональная академия безопасности и выживания", Орел, 2014 - (257 с.)  
<https://biblioclub.ru/index.php?page=book&id=428605;>
11. "2011-2012. Прогресс женщин мира. В стремлении к справедливости", Издательство: "Информационный центр ООН", 2011 - (168 с.)  
[https://biblioclub.ru/index.php?page=book&id=118478.](https://biblioclub.ru/index.php?page=book&id=118478)

## **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. Visual Studio;
6. MySQL;
7. Libre Office;
8. ERwin Data Modeler;
9. Bison;
10. ProjectLibre.

## **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](http://biblioclub.ru/index.php?page=main_ub_red)
3. Научная электронная библиотека - <https://elibrary.ru/>
4. База данных ВИНТИ 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. Электронная библиотека МЭИ (ЭБ МЭИ) - <http://elib.mpei.ru/login.php>
8. Портал открытых данных Российской Федерации - <https://data.gov.ru>

9. База открытых данных профессиональных стандартов Министерства труда и социальной защиты РФ - <http://profstandart.rosmintrud.ru/obshchiy-informatsionnyy-blok/natsionalnyy-reestr-professionalnykh-standartov/>

10. База открытых данных Министерства экономического развития РФ - <http://www.economy.gov.ru>

11. Национальный портал онлайн обучения «Открытое образование» - <https://openedu.ru>

## 6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Тип помещения	Номер аудитории, наименование	Оснащение
Учебные аудитории для проведения лекционных занятий и текущего контроля	Н-204, Учебная аудитория	парта со скамьей, стол преподавателя, стул, трибуна, доска меловая, колонки звуковые, мультимедийный проектор, экран
	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	М-509, Учебная лаборатория "Инженерно-техническая защита информации"	стол преподавателя, стул, стол письменный, мультимедийный проектор, экран, компьютер персональный, кондиционер, телевизор, стенд лабораторный
Учебные аудитории для проведения промежуточной аттестации	М-509, Учебная лаборатория "Инженерно-техническая защита информации"	стол преподавателя, стул, стол письменный, мультимедийный проектор, экран, компьютер персональный, кондиционер, телевизор, стенд лабораторный
	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
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

## БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА ДИСЦИПЛИНЫ

### Российские и международные стандарты информационной безопасности

(название дисциплины)

#### 8 семестр

#### Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:

КМ-1 КМ-1 (Контрольная работа)

КМ-2 КМ-2 (Контрольная работа)

КМ-3 КМ-3 (Контрольная работа)

КМ-4 КМ-4 (Контрольная работа)

Вид промежуточной аттестации – Экзамен.

Номер раздела	Раздел дисциплины	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
		Неделя КМ:	4	8	12	15
1	Зарубежные и международные стандарты в области информационной безопасности и их анализ					
1.1	Вводная лекция		+			
1.2	Тема 1.		+		+	
1.3	Тема 2.		+	+		
1.4	Тема 3.			+	+	
2	Национальные стандарты РФ в области информационной безопасности и их анализ					
2.1	Тема 4.				+	
2.2	Тема 5.		+			+
2.3	Тема 6.		+			+
2.4	Тема 7.		+	+		
3	Практика применения «Общих критериев» для разработки профилей защиты и заданий по безопасности информационных технологий					
3.1	Тема 8.		+	+	+	+
3.2	Тема 9.			+		+
3.3	Тема 10.			+	+	+

3.4	Тема 11.			+		
		Всего КМ, %:	20	20	30	30