

**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 компьютерных систем

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очная

**Рабочая программа дисциплины**  
**ТЕХНОЛОГИИ КОМПЬЮТЕРНОГО АУДИТА**

<b>Блок:</b>	<b>Блок 1 «Дисциплины (модули)»</b>
<b>Часть образовательной программы:</b>	<b>Часть, формируемая участниками образовательных отношений</b>
<b>№ дисциплины по учебному плану:</b>	<b>Б1.Ч.12</b>
<b>Трудоемкость в зачетных единицах:</b>	<b>7 семестр - 5;</b>
<b>Часов (всего) по учебному плану:</b>	<b>180 часов</b>
<b>Лекции</b>	<b>7 семестр - 32 часа;</b>
<b>Практические занятия</b>	<b>7 семестр - 48 часа;</b>
<b>Лабораторные работы</b>	<b>не предусмотрено учебным планом</b>
<b>Консультации</b>	<b>проводится в рамках часов аудиторных занятий</b>
<b>Самостоятельная работа</b>	<b>7 семестр - 99,7 часа;</b>
<b>в том числе на КП/КР</b>	<b>не предусмотрено учебным планом</b>
<b>Иная контактная работа</b>	<b>проводится в рамках часов аудиторных занятий</b>
<b>включая:</b>	
<b>Отчет</b>	
<b>Промежуточная аттестация:</b>	
<b>Зачет с оценкой</b>	<b>7 семестр - 0,3 часа;</b>

**Москва 2022**

## ПРОГРАММУ СОСТАВИЛ:

Преподаватель

(должность)

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

(подпись)

А.С. Минзов

(расшифровка  
подписи)

## СОГЛАСОВАНО:

Руководитель  
образовательной программы

(должность, ученая степень, ученое звание)

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

(подпись)

О.Р. Баронов

(расшифровка  
подписи)

Заведующий выпускающей  
кафедры

(должность, ученая степень, ученое звание)

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

(подпись)

А.Ю. Невский

(расшифровка  
подписи)

## 1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

**Цель освоения дисциплины:** сформировать у будущих специалистов систему понятий, знаний, умений и навыков в области аудита компьютерных систем

### Задачи дисциплины

- ознакомление студентов с нормативно-правовыми требованиями по проведению компьютерного аудита, а также его целями, принципами проведения и задачами;
- овладение технологиями сбора (добывания) информации об исследуемом объекте и оценке его защищенности;
- ознакомление с технологиями тестирования объекта исследования с использованием сканеров безопасности;
- развертывать и использовать ИТ для анализа событий на объекте исследования SIEM (ELK).

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-3 Способен администрировать средства защиты информации в компьютерных системах и сетях	ПК-3.1 <sub>ПК-3</sub> Администрирует подсистемы защиты информации в операционных системах	знать: - нормативно-правовые требования по проведению компьютерного аудита; - цели, принципы и методы проведения компьютерного аудита; - источники информации о защищенности компьютера; - технологии, применяемые при проведении компьютерного аудита; - этапы проведения аудита.  уметь: - определить конфигурацию рабочего места для проведения компьютерного аудита; - собрать (добыть) информацию об исследуемом объекте; - использовать технологии для оценки защищенности объекта исследования.
ПК-3 Способен администрировать средства защиты информации в компьютерных системах и сетях	ПК-3.3 <sub>ПК-3</sub> Администрирует средства защиты информации прикладного и системного программного обеспечения	знать: - назначение, принципы работы и технология анализа событий в исследуемом объекте; - основные технологии тестирования объекта исследования.  уметь: - развертывать и использовать ИТ для анализа событий на объекте исследования SIEM (ELK); - применять сканеры безопасности для оценки защищенности объекта исследования.

## **2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО**

Дисциплина относится к основной профессиональной образовательной программе Безопасность компьютерных 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 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	Раздел 1	26	7	6	-	10	-	-	-	-	-	10	-	<p><b><u>Подготовка к аудиторным занятиям:</u></b>                      Проработка лекции, выполнение и подготовка к защите лаб. работы  <b><u>Самостоятельное изучение теоретического материала:</u></b> Изучение дополнительного материала по разделу "Раздел 1"  <b><u>Подготовка к практическим занятиям:</u></b>                      Изучение материала по разделу "Раздел 1" подготовка к выполнению заданий на практических занятиях  <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 "Раздел 1" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам.  <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</p>	
1.1	Тема 1. Введение в дисциплину. Основные термины и определения	10		2	-	4	-	-	-	-	-	-	4		-
1.2	Тема 2. Нормативно-правовые требования по аудиту информационной безопасности. Виды аудита	16		4	-	6	-	-	-	-	-	-	6		-

													форме распечатанных презентационных слайдов. В качестве тем докладов студентам предлагаются следующие варианты: <b><u>Подготовка к текущему контролю:</u></b> Повторение материала по разделу "Раздел 1" <b><u>Изучение материалов литературных источников:</u></b> [1], 16-29 [2], 22-39	
2	Раздел 2	136	26	-	38	-	-	-	-	-	-	72	-	<b><u>Подготовка к текущему контролю:</u></b> Повторение материала по разделу "Раздел 2"
2.1	Тема 3. Этапы проведения аудита и используемые технологии	16	6	-	6	-	-	-	-	-	-	4	-	<b><u>Подготовка к аудиторным занятиям:</u></b> Проработка лекции, выполнение и подготовка к защите лаб. работы
2.2	Тема 4. Аудит информационных технологий с использованием сканеров безопасности	32	4	-	8	-	-	-	-	-	-	20	-	<b><u>Самостоятельное изучение теоретического материала:</u></b> Изучение дополнительного материала по разделу "Раздел 2" <b><u>Подготовка к практическим занятиям:</u></b> Изучение материала по разделу "Раздел 2"
2.3	Тема 5. Аудит событий на объекте исследования	88	16	-	24	-	-	-	-	-	-	48	-	подготовка к выполнению заданий на практических занятиях <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 предлагаются следующие варианты: <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 "Раздел 2" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных

													заданий. Проверка домашнего задания проводится по представленным письменным работам. <b><u>Изучение материалов литературных источников:</u></b> [1], 56-88
	Зачет с оценкой	18.0	-	-	-	-	-	-	-	0.3	-	17.7	
	Всего за семестр	180.0	32	-	48	-	-	-	-	0.3	82	17.7	
	Итого за семестр	180.0	32	-	48	-	-	-	-	0.3	99.7		

**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. Раздел 1

##### 1.1. Тема 1. Введение в дисциплину. Основные термины и определения

Цели и задачи дисциплины. Рабочая программа проведения дисциплины и система контроля знаний с использованием платформы Moodle. Организация проведения практических занятий. Требования к уровню достигаемых компетенций в области технологий проведения компьютерного аудита. Способы контроля знаний и критерии определения оценок. Основные термины и определения: компьютерный аудит, сканер безопасности, пен-тестирование, системы управления событиями (SIEM). Методы и технологии организации рабочего места для проведения тестирования..

##### 1.2. Тема 2. Нормативно-правовые требования по аудиту информационной безопасности. Виды аудита

ГОСТ Р ИСО/МЭК 27007-2014 Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности. Разработка целей и задач аудита компьютерной безопасности. Определение программы аудита. Идентификация и оценка рисков программы аудита. Идентификация ресурсов для программы аудита. Критерии аудита и форма представления его результатов. Обоснование методов проведения компьютерного аудита..

#### 2. Раздел 2

##### 2.1. Тема 3. Этапы проведения аудита и используемые технологии

Организация проведения компьютерного аудита. Подготовка к проведению аудита и сбор информации об объектах исследования со стороны внешней среды. Разработка программы аудита. Этапы проведения аудита. Обработка результатов и подготовка отчета. Разработка выводов и рекомендаций по результатам компьютерного аудита. Анализ защищенности с использованием средств операционных систем и утилит..

##### 2.2. Тема 4. Аудит информационных технологий с использованием сканеров безопасности

Классификация сканеров безопасности. Краткая характеристика наиболее популярных из них. Практическая работа по освоению сканеров безопасности WindowsVulnerabilityScanner, Nessus, Nmap. Методика анализа результатов сканирования. Технологии организации и проведения тестирования на проникновение..

##### 2.3. Тема 5. Аудит событий на объекте исследования

Понятие «событие» в системе информационной безопасности. Технологии анализа событий DLP, SIEM, TrafficMonitors. Развертывание системы ELKStack. Анализ событий на исследуемом объекте. Разработка отчета с выводами по защищенности исследуемого объекта.

### **3.3. Темы практических занятий**

1. 2. Настройка журнала событий в ОС Windows для проведения компьютерного аудита.;
2. 8. Установка системы мониторинга событий в ELK и практическая работа по аудиту событий.;
3. 7. Технология работы с утилитой auditv ELK.;
4. 6. Анализ и визуализация журналов событий на исследуемом объекте с



использованием ELK.;

5. 5. Развертывание и первичная настройка ELK.;

6. 4. Анализ защищенности объекта исследований с использованием сканеров безопасности.;

7. 3. Технологии сбора информации об исследуемом объекте аудита из открытых источников.;

8. 1. Конфигурация рабочего места для проведения компьютерного аудита..

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

### **3.5 Консультации**

#### *Групповые консультации по разделам дисциплины (ГК)*

1. Обсуждение материалов по кейсам раздела "Раздел 1"
2. Обсуждение материалов по кейсам раздела "Раздел 2"

#### *Текущий контроль (ТК)*

1. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Раздел 1"
2. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Раздел 2"

### **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	
<b>Знать:</b>				
этапы проведения аудита	ПК-3.1 <sub>ПК-3</sub>	+		Отчет/Задание 1; Задание 2
технологии, применяемые при проведении компьютерного аудита	ПК-3.1 <sub>ПК-3</sub>		+	Отчет/Задание 5; Задание 6
источники информации о защищенности компьютера	ПК-3.1 <sub>ПК-3</sub>	+		Отчет/Задание 1; Задание 2
цели, принципы и методы проведения компьютерного аудита	ПК-3.1 <sub>ПК-3</sub>		+	Отчет/Задание 7; Задание 8
нормативно-правовые требования по проведению компьютерного аудита	ПК-3.1 <sub>ПК-3</sub>		+	Отчет/Задание 3; Задание 4
основные технологии тестирования объекта исследования	ПК-3.3 <sub>ПК-3</sub>		+	Отчет/Задание 7; Задание 8
назначение, принципы работы и технология анализа событий в исследуемом объекте	ПК-3.3 <sub>ПК-3</sub>		+	Отчет/Задание 3; Задание 4
<b>Уметь:</b>				
использовать технологии для оценки защищенности объекта исследования	ПК-3.1 <sub>ПК-3</sub>	+		Отчет/Задание 1; Задание 2
собрать (добыть) информацию об исследуемом объекте	ПК-3.1 <sub>ПК-3</sub>		+	Отчет/Задание 3; Задание 4
определить конфигурацию рабочего места для проведения компьютерного аудита	ПК-3.1 <sub>ПК-3</sub>		+	Отчет/Задание 3; Задание 4
применять сканеры безопасности для оценки защищенности объекта исследования	ПК-3.3 <sub>ПК-3</sub>		+	Отчет/Задание 5; Задание 6
развертывать и использовать ИТ для анализа событий на объекте исследования SIEM (ELK)	ПК-3.3 <sub>ПК-3</sub>		+	Отчет/Задание 7; Задание 8

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

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

**7 семестр**

Форма реализации: Проверка задания

1. Задание 1; Задание 2 (Отчет)
2. Задание 3; Задание 4 (Отчет)
3. Задание 5; Задание 6 (Отчет)
4. Задание 7; Задание 8 (Отчет)

Балльно-рейтинговая структура дисциплины является приложением А.

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

*Зачет с оценкой (Семестр №7)*

Оценка определяется по совокупности результатов текущего контроля успеваемости в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ»

В диплом выставляется оценка за 7 семестр.

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

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

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

1. Управление событиями информационной безопасности : учебное пособие / А. С. Минзов, О. Р. Баронов, С. А. Минзов, П. А. Осипов, Нац. исслед. ун-т "МЭИ" (НИУ"МЭИ"), Инженерно-экономич. ин-т национального исслед. ун-та "МЭИ" ; ред. А. Ю. Невский . – Москва : ВНИИгеосистем, 2020 . – 110 с. - Для студентов бакалавриата, магистратуры, аспирантов и преподавателей, занимающихся вопросами создания эффективных систем управления кибербезопасностью . - ISBN 978-5-8481-0244-4 .;
2. В. И. Подольский, Н. С. Щербакова, В. Л. Комиссаров- "Компьютерные информационные системы в аудите", Издательство: "Юнити", Москва, 2015 - (160 с.)  
<https://biblioclub.ru/index.php?page=book&id=115315>.

### **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](http://biblioclub.ru/index.php?page=main_ub_red)
3. Научная электронная библиотека - <https://elibrary.ru/>

4. База данных Web of Science - <http://webofscience.com/>
5. База данных Scopus - <http://www.scopus.com>
6. Национальная электронная библиотека - <https://rusneb.ru/>
7. ЭБС "Консультант студента" - <http://www.studentlibrary.ru/>
8. Журналы Журналы Royal Society of Chemistry - <https://pubs.rsc.org/>
9. Журналы издательства SAGE Publication (Sage) - <https://journals.sagepub.com/>
10. Журнал Science - <https://www.sciencemag.org/>
11. Электронная библиотека МЭИ (ЭБ МЭИ) - <http://elib.mpei.ru/login.php>
12. Портал открытых данных Российской Федерации - <https://data.gov.ru>
13. База открытых данных Министерства труда и социальной защиты РФ - <https://rosmintrud.ru/opendata>
14. База открытых данных профессиональных стандартов Министерства труда и социальной защиты РФ - <http://profstandart.rosmintrud.ru/obshchiy-informatsionnyy-blok/natsionalnyy-reestr-professionalnykh-standartov/>
15. База открытых данных Министерства экономического развития РФ - <http://www.economy.gov.ru>
16. База открытых данных Росфинмониторинга - <http://www.fedsfm.ru/opendata>
17. Электронная открытая база данных "Polpred.com Обзор СМИ" - <https://www.polpred.com>
18. Национальный портал онлайн обучения «Открытое образование» - <https://openedu.ru>
19. Официальный сайт Федерального агентства по техническому регулированию и метрологии - <http://protect.gost.ru/>
20. Открытая университетская информационная система «РОССИЯ» - <https://uisrussia.msu.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	3-512, Учебная аудитория	парта, стол преподавателя, стул, доска меловая
Учебные аудитории для проведения промежуточной аттестации	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
	3-512, Учебная аудитория	парта, стол преподавателя, стул, доска меловая
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****Технологии компьютерного аудита**

(название дисциплины)

**7 семестр****Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:**

КМ-1 Задание 1; Задание 2 (Отчет)

КМ-2 Задание 3; Задание 4 (Отчет)

КМ-3 Задание 5; Задание 6 (Отчет)

КМ-4 Задание 7; Задание 8 (Отчет)

**Вид промежуточной аттестации – Зачет с оценкой.**

Номер раздела	Раздел дисциплины	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
		Неделя КМ:	4	8	12	15
1	Раздел 1					
1.1	Тема 1. Введение в дисциплину. Основные термины и определения		+			
1.2	Тема 2. Нормативно-правовые требования по аудиту информационной безопасности. Виды аудита		+			
2	Раздел 2					
2.1	Тема 3. Этапы проведения аудита и используемые технологии			+		
2.2	Тема 4. Аудит информационных технологий с использованием сканеров безопасности			+		
2.3	Тема 5. Аудит событий на объекте исследования				+	+
Вес КМ, %:			25	25	25	25