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

Блок:	**Блок 1 «Дисциплины (модули)»**
Часть образовательной программы:	**Вариативная**
№ дисциплины по учебному плану:	**Б1.В.09.06.01**
Трудоемкость в зачетных единицах:	**8 семестр - 4;**
Часов (всего) по учебному плану:	**144 часа**
Лекции	**8 семестр - 28 часа;**
Практические занятия	**8 семестр - 28 часа;**
Лабораторные работы	**не предусмотрено учебным планом**
Консультации	**8 семестр - 2 часа;**
Самостоятельная работа	**8 семестр - 85,5 часа;**
в том числе на КП/КР	**не предусмотрено учебным планом**
Иная контактная работа	**проводится в рамках часов аудиторных занятий**
включая: **Семинар**	
Промежуточная аттестация:	
Экзамен	**8 семестр - 0,5 часа;**

Москва 2018

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:

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: овладение компетенциями, связанными с овладением современными приемами и методами аудита безопасности информационных систем организаций на основе использования программных средств и методов активного аудита

Задачи дисциплины

- изучение роли, места и технологии проведения аудита в системе менеджмента информационной безопасности (СМИБ);
- освоение приемов, способов и технологии компьютерного аудита информационной системы организации;
- приобретение опыта проведения работ основных этапов аудита, анализа его результатов в целях принятия управленческих решений.

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 способностью администрировать подсистемы информационной безопасности объекта защиты		знать: - перечень и содержание информации аудита, получаемой из программных приложений; - перечень и возможности программных приложений по выполнению основных функций аудита, включая open source решения. уметь: - применять результаты анализа информации аудита для принятия управленческих решений в информационной системе организации; - выполнять перечень операций по работе с программными приложениями, выполняющими функции аудита, включая open source решения.
ПК-10 способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности		знать: - перечень и содержание стандартов серии ГОСТ Р ИСО/МЭК 27000 в области аудита информационной безопасности; - перечень и содержание требований руководящих документов к аудиту некоторых информационных систем: ИСПДН, КИИ, ГИС. уметь: - разработать и реализовать план проведения аудита информационной системы организации; - разработать и корректировать план выполнения требований руководящих документов по обеспечению

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Запланированные результаты обучения
		безопасности информационных систем на основе данных аудита.
ПСК-1 Способность администрировать подсистемы информационной безопасности объектов, объекты энергетики КВО РФ, эксплуатирующие АСУ ТП		знать: - основы аудита безопасности информационных систем, включая отраслевые системы (объекты энергетики, относящиеся к КВО РФ); - возможности компьютерного аудита, встроенные в операционные системы, базы данных и другие программные приложения. уметь: - проводить анализ сведений аудита, получаемых из программных приложений, включая и используемые в отраслевых системах (объекты энергетики, относящиеся к КВО РФ); - настраивать приложения аудита, встроенные в операционные системы, базы данных и другие программные комплексы.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к части, формируемой участниками образовательных отношений блока дисциплин 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 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	Теоретические основы компьютерного аудита безопасности информационных систем	38	8	8	-	8	-	-	-	-	-	22	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Теоретические основы компьютерного аудита безопасности информационных систем"
1.1	Теоретические основы компьютерного аудита безопасности информационных систем	38		8	-	8	-	-	-	-	-	22	-	***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы ***Подготовка домашнего задания:*** Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Теоретические основы компьютерного аудита безопасности информационных систем" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам. ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Теоретические основы компьютерного аудита безопасности информационных систем" подготовка к выполнению заданий на практических занятиях ***Самостоятельное изучение теоретического материала:*** Изучение

														дополнительного материала по разделу "Теоретические основы компьютерного аудита безопасности информационных систем" ***Изучение материалов литературных источников:*** [1], 56-88
2	Технологии компьютерного аудита	70		20	-	20	-	-	-	-	-	30	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Технологии компьютерного аудита"
2.1	Технологии компьютерного аудита	70		20	-	20	-	-	-	-	-	30	-	***Подготовка домашнего задания:*** Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Технологии компьютерного аудита" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам. ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Технологии компьютерного аудита" подготовка к выполнению заданий на практических занятиях ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Технологии компьютерного аудита" ***Изучение материалов литературных источников:*** [1], 16-29 [2], 22-39
	Экзамен	36.0		-	-	-	-	2	-	-	0.5	-	33.5	
	Всего за семестр	**144.0**		**28**	**-**	**28**	**-**	**2**	**-**	**-**	**0.5**	**52**	**33.5**	
	Итого за семестр	**144.0**		**28**	**-**	**28**	**2**		**-**		**0.5**	**85.5**		

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. Теоретические основы компьютерного аудита безопасности информационных систем

1.1. Теоретические основы компьютерного аудита безопасности информационных систем

Понятие, цели. виды, назначение аудита безопасности информационных систем. Традиционный аудит, активный аудит. Роль и место аудита в системе менеджмента информационной безопасности (СМИБ). Положения ГОСТ Р ИСО/МЭК 27000 по аудиту безопасности. Основные положения стандартов ГОСТ Р ИСО/МЭК 27007-2014 и ГОСТ Р 56045-2014/ISO/IEC TR 27008:2011 по последовательности проведения аудита. Особенности проведения компьютерного аудита и получения свидетельств, измерений и фактов. Основы анализа информации аудита, ее представление в отчетах. Визуализация информации аудита. Формирование и принятие управленческих решений на основе информации аудита..

2. Технологии компьютерного аудита

2.1. Технологии компьютерного аудита

Средства аудита встроенные в программные приложения: операционные системы и прикладные программы. Программные приложения и практика их применение для аудита безопасности: сканеры безопасности, DLP-системы, SIEM-системы. Решения open source для проведения аудита: утилита n-map, Metasploit Framework. Практикум работы по аудиту безопасности. Технология обработки данных аудита. Аналитические возможности аудитора и программного обеспечения. Требования к отчету по результатам аудита. Формирование отчетов аудита безопасности..

3.3. Темы практических занятий

1. Конфигурация рабочего места для проведения компьютерного аудита;
2. Настройка журнала событий в ОС Windowsдля проведения компьютерного аудита;
3. Технологии сбора информации об исследуемом объекте аудита из открытых источников;
4. Анализ защищенности объекта исследований с использованием сканеров безопасности;
5. Развертывание и первичная настройка ELK;
6. Анализ и визуализация журналов событий на исследуемом объекте с использованием ELK;
7. Технология работы с утилитой auditв ELK;
8. Установка системы мониторинга событий в ELKи практическая работа по аудиту событий.

3.4. Темы лабораторных работ

не предусмотрено

3.5 Консультации

Групповые консультации по разделам дисциплины (ГК)

1. Обсуждение материалов по кейсам раздела "Теоретические основы компьютерного аудита безопасности информационных систем"
2. Обсуждение материалов по кейсам раздела "Технологии компьютерного аудита"

Текущий контроль (ТК)

1. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Теоретические основы компьютерного аудита безопасности информационных систем"
2. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Технологии компьютерного аудита"

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	
Знать:				
перечень и возможности программных приложений по выполнению основных функций аудита, включая open source решения	ПК-3(Компетенция)		+	Семинар/КМ-4
перечень и содержание информации аудита, получаемой из программных приложений	ПК-3(Компетенция)		+	Семинар/КМ-5
перечень и содержание требований руководящих документов к аудиту некоторых информационных систем: ИСПДН, КИИ, ГИС	ПК-10(Компетенция)	+		Семинар/КМ-1
перечень и содержание стандартов серии ГОСТ Р ИСО/МЭК 27000 в области аудита информационной безопасности	ПК-10(Компетенция)	+		Семинар/КМ-1
возможности компьютерного аудита, встроенные в операционные системы, базы данных и другие программные приложения	ПСК-1(Компетенция)	+		Семинар/КМ-2
основы аудита безопасности информационных систем, включая отраслевые системы (объекты энергетики, относящиеся к КВО РФ)	ПСК-1(Компетенция)	+		Семинар/КМ-3
Уметь:				
выполнять перечень операций по работе с программными приложениями, выполняющими функции аудита, включая open source решения	ПК-3(Компетенция)		+	Семинар/КМ-3
применять результаты анализа информации аудита для принятия управленческих решений в информационной системе организации	ПК-3(Компетенция)		+	Семинар/КМ-4
разработать и корректировать план выполнения требований руководящих документов по обеспечению безопасности информационных систем на основе данных аудита	ПК-10(Компетенция)		+	Семинар/КМ-5
разработать и реализовать план проведения аудита информационной системы организации	ПК-10(Компетенция)		+	Семинар/КМ-5
настраивать приложения аудита, встроенные в операционные системы, базы данных и другие программные комплексы	ПСК-1(Компетенция)	+		Семинар/КМ-1

проводить анализ сведений аудита, получаемых из программных приложений, включая и используемые в отраслевых системах (объекты энергетики, относящиеся к КВО РФ)	ПСК-1(Компетенция)	+		Семинар/КМ-2

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: Проверка задания

1. КМ-1 (Семинар)
2. КМ-2 (Семинар)
3. КМ-3 (Семинар)
4. КМ-4 (Семинар)
5. КМ-5 (Семинар)

Балльно-рейтинговая структура дисциплины является приложением А.

4.2 Промежуточная аттестация по дисциплине

Экзамен (Семестр №8)

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

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. Петренко, С. А. Аудит безопасности Intranet / С. А. Петренко, А. А. Петренко . – М. : ДМК Пресс, 2002 . – 416 с. – (Информационные технологии для инженеров) . - ISBN 5-940741-83-5 .;
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
3. **Научная электронная библиотека** - https://elibrary.ru/
4. **Национальная электронная библиотека** - https://rusneb.ru/

5. **ЭБС "Консультант студента"** - http://www.studentlibrary.ru/
6. **Электронная библиотека МЭИ (ЭБ МЭИ)** - http://elib.mpei.ru/login.php
7. **Портал открытых данных Российской Федерации** - https://data.gov.ru
8. **База открытых данных Министерства труда и социальной защиты РФ** - https://rosmintrud.ru/opendata
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. **База открытых данных Росфинмониторинга** - http://www.fedsfm.ru/opendata
12. **Электронная открытая база данных "Polpred.com Обзор СМИ"** - https://www.polpred.com
13. **Информационно-справочная система «Кодекс/Техэксперт»** - Http:\\proinfosoft.ru; http://docs.cntd.ru/
14. **Национальный портал онлайн обучения «Открытое образование»** - https://openedu.ru
15. **Официальный сайт Федерального агентства по техническому регулированию и метрологии** - http://protect.gost.ru/
16. **Открытая университетская информационная система «РОССИЯ»** - https://uisrussia.msu.ru
17. **Официальный сайт Министерства науки и высшего образования Российской Федерации** - https://minobrnauki.gov.ru
18. **Официальный сайт Федеральной службы по надзору в сфере образования и науки** - https://obrnadzor
19. **Федеральный портал "Российское образование"** - http://www.edu.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-508, Учебная аудитория	парта со скамьей, стол преподавателя, стул, доска меловая
Учебные аудитории для проведения лабораторных занятий	М-508, Учебная аудитория	парта со скамьей, стол преподавателя, стул, доска меловая
Учебные аудитории для проведения промежуточной аттестации	М-508, Учебная аудитория	парта со скамьей, стол преподавателя, стул, доска меловая
	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	М-508, Учебная	парта со скамьей, стол преподавателя,

консультирования	аудитория	стул, доска меловая
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

Технологии компьютерного аудита

(название дисциплины)

8 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:
КМ-1 КМ-1 (Семинар)
КМ-2 КМ-2 (Семинар)
КМ-3 КМ-3 (Семинар)
КМ-4 КМ-4 (Семинар)
КМ-5 КМ-5 (Семинар)

Вид промежуточной аттестации – Экзамен.

Номер раздела	Раздел дисциплины	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4	КМ-5
		Неделя КМ:	2	4	8	12	15
1	Теоретические основы компьютерного аудита безопасности информационных систем						
1.1	Теоретические основы компьютерного аудита безопасности информационных систем		+	+	+		
2	Технологии компьютерного аудита						
2.1	Технологии компьютерного аудита				+	+	+
		Вес КМ, %:	10	20	20	20	30