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: Очно-заочная

Рабочая программа дисциплины
АУДИТ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Блок:	**Блок 1 «Дисциплины (модули)»**
Часть образовательной программы:	**Часть, формируемая участниками образовательных отношений**
№ дисциплины по учебному плану:	**Б1.Ч.03**
Трудоемкость в зачетных единицах:	**9 семестр - 6;**
Часов (всего) по учебному плану:	**216 часов**
Лекции	**9 семестр - 16 часов;**
Практические занятия	**9 семестр - 20 часов;**
Лабораторные работы	**не предусмотрено учебным планом**
Консультации	**9 семестр - 10 часов;**
Самостоятельная работа	**9 семестр - 165,2 часа;**
в том числе на КП/КР	**9 семестр - 15,7 часов;**
Иная контактная работа	**9 семестр - 4 часа;**
включая: **Тестирование** **Контрольная работа** **Коллоквиум**	
Промежуточная аттестация:	
Экзамен **Защита курсовой работы**	**9 семестр - 0,5 часа;** **9 семестр - 0,3 часа;** **всего - 0,8 часа**

Москва 2026

ПРОГРАММУ СОСТАВИЛ:

Преподаватель	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Писаренко И.В. Идентификатор: R2828e375-PisarenkoIV-105ccd67	И.В. Писаренко

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Баронов О.Р. Идентификатор: R90d76356-BaronovOR-7bf8fd7e	О.Р. Баронов
Заведующий выпускающей кафедрой	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Невский А.Ю. Идентификатор: R4bc65573-NevskyAY-0b6e493d	А.Ю. Невский

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель освоения дисциплины: изучение теоретических основ и получение практических навыков по организации и проведению аудита безопасности информационных систем предприятия.

Задачи дисциплины

- −изучение теоретических основ и проведения аудита безопасности информационных систем на предприятии (в организации);
- −рассмотрение основных способов и методов оценивания состояния информационной безопасности;
- −приобретение практических навыков в проведении оценок соответствия информационной безопасности с использованием специализированного программного обеспечения.

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**
РПК-1 Готов обеспечивать защиту информации в автоматизированных системах в процессе их эксплуатации	ИД-З$_{РПК-1}$ Выполняет мониторинг защищенности информации в автоматизированных системах	знать: - –основы менеджмента безопасности информационных систем;; - –требования нормативных и правовых документов (законы, стандарты, регламенты) в предметной области дисциплины;. уметь: - –проводить мероприятия по управлению программой безопасности информационных систем;; - –разрабатывать и управлять программой аудита безопасности информационных систем;.
РПК-1 Готов обеспечивать защиту информации в автоматизированных системах в процессе их эксплуатации	ИД-4$_{РПК-1}$ Выполняет аудит защищенности информации в автоматизированных системах	знать: - –особенности практической организации и проведения аудита безопасности информационных систем.; - –основы аудита безопасности информационных систем;. уметь: - –осуществлять оценку соответствия информационной безопасности предприятия;; - –оформлять необходимые документы в рамках аудита безопасности информационных систем.; - –проводить основные организационные мероприятия по проведению аудита безопасности информационных систем;.

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 6 зачетных единиц, 216 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	Вводная лекция	12	9	1	-	1	-	-	-	-	-	10	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Вводная лекция" ***Подготовка к аудиторным занятиям:*** Проработка лекции ***Изучение материалов литературных источников:*** [1], 1-55с [2], 1-299 [3], 1-416
1.1	Понятие и виды аудита информационной безопасности	12		1	-	1	-	-	-	-	-	10	-	
2	Менеджмент аудита безопасности информационных систем	43		6	-	6	-	-	-	-	-	31	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Менеджмент аудита безопасности информационных систем" ***Подготовка к аудиторным занятиям:*** Проработка лекции ***Подготовка домашнего задания:*** Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Менеджмент аудита безопасности информационных систем" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам.
2.1	Правовые основы аудита информационной безопасности	6		1	-	1	-	-	-	-	-	4	-	
2.2	Способы и цели контроля и проверки процессов и систем	7		1	-	1	-	-	-	-	-	5	-	
2.3	Виды аудита информационной безопасности	10		1	-	1	-	-	-	-	-	8	-	
2.4	Менеджмент аудита информационной безопасности	12		2	-	2	-	-	-	-	-	8	-	
2.5	Программа аудита	8		1	-	1	-	-	-	-	-	6	-	

	информационной безопасности													***Подготовка доклада, выступления:*** 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: ***Подготовка к контрольной работе:*** Изучение материалов по разделу Менеджмент аудита безопасности информационных систем и подготовка к контрольной работе ***Подготовка курсовой работы:*** Курсовая работа представлена в виде крупной задачи по учебному кейсу, охватывающей несколько расчетных вопросов и выбор варианта проектного решения. Пример задания: ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Менеджмент аудита безопасности информационных систем" подготовка к выполнению заданий на практических занятиях ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Менеджмент аудита безопасности информационных систем" ***Подготовка расчетных заданий:*** Задания ориентированы на решения минизадач по разделу "Менеджмент аудита безопасности информационных систем". Студенты необходимо повторить теоретический материал, разобрать примеры решения аналогичных задач. провести расчеты по варианту задания и сделать выводы. В качестве задания используются следующие

														упражнения: Разработка программы аудита информационной безопасности, разработка плана аудита информационной безопасности. ***<u>Подготовка реферата:</u>*** В рамках реферативной части студенту необходим провести обзор литературных источников по выбранной теме, комплексно осветить вопрос в соответствии с темой реферата, подготовить презентацию для выступления по результатам работы на семинарском занятии. В качестве тем реферата студенту предлагаются следующие варианты: ***<u>Изучение материалов литературных источников:</u>*** [3], 1-416 [5], 1-176
3	Особенности проведения аудита безопасности информационных систем	97		9	-	13	-	-	-	-	-	75	-	***<u>Подготовка к текущему контролю:</u>*** Повторение материала по разделу "Особенности проведения аудита безопасности информационных систем" ***<u>Подготовка к аудиторным занятиям:</u>*** Проработка лекции ***<u>Подготовка домашнего задания:</u>*** Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Особенности проведения аудита безопасности информационных систем" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам. ***<u>Подготовка доклада, выступления:</u>*** Задание связано с углубленным изучением разделов дисциплины и самостоятельным поиском материалов для раскрытия темы
3.1	Основные этапы аудита информационной безопасности	8		1	-	1	-	-	-	-	-	6	-	
3.2	Проведение аудита информационной безопасности	45		2	-	4	-	-	-	-	-	39	-	
3.3	Способы оценки информационной безопасности	8		2	-	4	-	-	-	-	-	2	-	
3.4	Модели оценки информационной безопасности	8		1	-	1	-	-	-	-	-	6	-	
3.5	Аудит управления непрерывностью бизнеса	8		1	-	1	-	-	-	-	-	6	-	
3.6	Проведение аудита	12		1	-	1	-	-	-	-	-	10	-	

	информационной безопасности в организациях банковской системы России													доклада. Материалы выполненной работы представляются в электронном виде или в форме распечатанных презентационных слайдов. В качестве тем докладов студентам предлагаются следующие варианты:
3.7	Проведение категорирования и аудита информационной безопасности объектов критической информационной инфраструктуры	8		1	-	1	-	-	-	-	-	6	-	***Подготовка к контрольной работе:*** Изучение материалов по разделу Особенности проведения аудита безопасности информационных систем и подготовка к контрольной работе ***Подготовка курсовой работы:*** Курсовая работа представлена в виде крупной задачи по учебному кейсу, охватывающей несколько расчетных вопросов и выбор варианта проектного решения. Пример задания: ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Особенности проведения аудита безопасности информационных систем" подготовка к выполнению заданий на практических занятиях ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Особенности проведения аудита безопасности информационных систем" ***Подготовка расчетных заданий:*** Задания ориентированы на решения минизадач по разделу "Особенности проведения аудита безопасности информационных систем". Студенты необходимо повторить теоретический материал, разобрать примеры решения аналогичных задач. провести расчеты по варианту задания и сделать выводы. В качестве задания используются следующие упражнения: Проведение оценки информационной безопасности по СТО БР ИББС 1.0-2014, по отдельным групповым показателям.

														Подготовка реферата: В рамках реферативной части студенту необходим провести обзор литературных источников по выбранной теме, комплексно осветить вопрос в соответствии с темой реферата, подготовить презентацию для выступления по результатам работы на семинарском занятии. В качестве тем реферата студенту предлагаются следующие варианты: ***Изучение материалов литературных источников:*** [4], 1-256
	Экзамен	36.0		-	-	-	-	2	-	-	0.5	-	33.5	
	Курсовая работа (КР)	28.0		-	-	-	8	-	4	-	0.3	15.7	-	
	Всего за семестр	**216.0**		**16**	**-**	**20**	**8**	**2**	**4**	**-**	**0.8**	**131.7**	**33.5**	
	Итого за семестр	**216.0**		**16**	**-**	**20**	**10**		**4**		**0.8**	**165.2**		

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. Вводная лекция

1.1. Понятие и виды аудита информационной безопасности

1.Аудит информационной безопасности — необходимый инструмент обеспечения информационной безопасности. 2.Понятие аудита информационной безопасности.

2. Менеджмент аудита безопасности информационных систем

2.1. Правовые основы аудита информационной безопасности

1.Правовое регулирование аудита информационной безопасности в Российской Федерации. 2.Международное законодательство в области аудита информационной безопасности. 3.Стандарты, используемые при проведении аудита безопасности информационных систем в Российской Федерации.

2.2. Способы и цели контроля и проверки процессов и систем

1.Оценка процессов — основа контроля и проверки процессов и систем. 2.Определение входных данных оценки. 3. Роли и обязанности по проведению оценивания 4. Модель оценки процесса 5. Мероприятия процесса оценивания и выходные данные оценивания 6. Факторы успешной оценки процесса.

2.3. Виды аудита информационной безопасности

1.Основные направления аудита ИБ. 2.Виды аудита ИБ.

2.4. Менеджмент аудита информационной безопасности

1.Процессная модель аудита информационной безопасности. 2.Менеджмент аудита информационной безопасности.

2.5. Программа аудита информационной безопасности

1.Программа аудита информационной безопасности. Управление программой аудита информационной безопасности. 2.Планирование программы аудита информационной безопасности.

3. Особенности проведения аудита безопасности информационных систем

3.1. Основные этапы аудита информационной безопасности

1.Основные этапы проведения аудита информационной безопасности. 2.Организация проведения аудита информационной безопасности. 3.Подготовка к проведению аудита информационной безопасности на месте. 4. Разработка плана проведения аудита информационной безопасности.

3.2. Проведение аудита информационной безопасности

1.Проведение аудита информационной безопасности на месте. 2.Сбор и оценка полученных данных 3.Подготовка и рассылка отчета по аудиту. 4.Завершение аудита информационной безопасности.

3.3. Способы оценки информационной безопасности

1.Способы оценки информационной безопасности. 2.Измерение эффективности системы менеджмента информационной безопасности.

3.4. Модели оценки информационной безопасности

1.Оценивание информационной безопасности на основе показателей информационной безопасности. 2.Оценивание информационной безопасности на основе моделей зрелости процессов обеспечения информационной безопасности.

3.5. Аудит управления непрерывностью бизнеса

1.Непрерывность бизнеса. 2.Аудит управления непрерывностью бизнеса и восстановления после сбоев.

3.6. Проведение аудита информационной безопасности в организациях банковской системы России

1.Стандарты Банка России СТО БР ИББС. 2.Серия ГОСТ 57580. 3.Нормативные документы Банка России.

3.7. Проведение категорирования и аудита информационной безопасности объектов критической информационной инфраструктуры

1.Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуре РФ». 2.Категорирование объектов критической информационной инфраструктуры. 3.Соблюдение требований федерального законодательства о безопасности критической информационной инфраструктуры.

3.3. Темы практических занятий

1. 8.Использование специализированного программного обеспечения аудита информационной безопасности на примере ПО Estimate Tools;
2. 7.Отчетность по аудиту безопасности информационных систем. Подготовка отчета и заключения по аудиту;
3. 6.Сканирование на уязвимости, тесты на проникновение. Особенности проведения и использования полученных результатов;
4. 5.Активный аудит информационной безопасности: виды, методы, используемые средства;
5. 4.Особенности проведения работ в ходе аудита безопасности информационных систем;
6. 3.План и программа аудита безопасности информационных систем. Менеджмент программа аудита;
7. 2.Международный стандарт ISO 19011. Руководящие указания по аудиту систем менеджмента. Комплекс стандартов Банка России СТО БР ИББС «Обеспечение информационной безопасности организаций банковской системы Российской Федерации»;
8. 1.Способы контроля и проверки процессов информационных систем. Цели контроля и проверки процессов и систем.

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 "Вводная лекция"
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 "Менеджмент аудита безопасности информационных систем"
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 "Особенности проведения аудита безопасности информационных систем"

Индивидуальные консультации по курсовому проету /работе (ИККП)

1. Консультации проводятся по разделу "Вводная лекция"
2. Консультации проводятся по разделу "Менеджмент аудита безопасности информационных систем"
3. Консультации проводятся по разделу "Особенности проведения аудита безопасности информационных систем"

Текущий контроль (ТК)

1. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Вводная лекция"
2. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Менеджмент аудита безопасности информационных систем"
3. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Особенности проведения аудита безопасности информационных систем"

3.6 Тематика курсовых проектов/курсовых работ

9 Семестр

Курсовая работа (КР)

Темы:

- Анализ законодательства Российской Федерации в области аудиторской деятельности.
- Анализ зарубежного законодательства в области аудита информационной безопасности.
- Требования национальных и международных нормативных актов, предписывающих и регламентирующих проведение инструментального контроля в коммерческом банке.
- Организационные аспекты проведения внешнего теста на проникновение в коммерческом банке.
- Особенности планирования и внедрения программы аудита информационной безопасности.
- Особенности контроля и совершенствования программы аудита информационной безопасности.
- Разработка плана аудита ИБ для коммерческого банка (СТО БР ИББС 1.0-2014).
- Разработка плана аудита ИБ для коммерческого банка (Положение БР № 382-П).
- Разработка плана аудита ИБ для коммерческого банка (ПП-1119).
- Основные технические отличия процесса обнаружения уязвимостей и теста на проникновение.
- Методы и техники, применяемые на этапе сбора информации («reconnaissance») о коммерческом банке при подготовке теста на проникновение.
- Состав и содержание мероприятий, проводимых на различных этапах теста на проникновение в коммерческом банке.
- Обзор и сравнение существующих баз данных уязвимостей ИБ (национальных и международных), применимых для использования в коммерческом банке.

- Поиск и анализ уязвимостей в web-приложениях коммерческого банка при помощи средств инструментального аудита.
- Завершение аудита информационной безопасности (провести анализ проводимых мероприятий).
- Особенности проведения аудита информационной безопасности в банковской сфере.
- Проведение аудита непрерывности бизнеса для коммерческой организации.
- Организационные и технические аспекты написания отчета о проведении теста на проникновение.
- Возможные направления деятельности «Red Team» в коммерческом банке
- Компетентность и оценка аудиторов в области информационной безопасности. Составить профиль аудитора информационной безопасности.
- Анализ требований стандарта COBIT по вопросам проведения аудита информационной безопасности.
- Анализ требований комплекса стандартов Банка России по проведению аудита информационной безопасности.
- Анализ требований стандартов ГОСТ Р ИСО\МЭК 270xx по проведению аудита информационной безопасности.
- Классификация аудита информационной безопасности (провести анализ признаков классификации).
- Анализ основных способов и методов проведения аудита информационной безопасности.
- Концептуальная схема аудита информационной безопасности. Цели и задачи аудита.
- Основные типовые ситуации, при которых возникает необходимость в проведении аудита информационной безопасности.
- Принципы аудита информационной безопасности. Реализация принципов на практике.
- Составить и обосновать модель оценки процесса обеспечения информационной безопасности.
- Роли и обязанности аудиторской группы в ходе аудита информационной безопасности.
- Анализ мероприятий процесса оценки информационной безопасности.
- Программа аудита информационной безопасности. Управление программой аудита информационной безопасности.
- Разработка программы аудита ИБ для коммерческого банка.
- Осознание аудита информационной безопасности. Роль руководства организации и службы информационной безопасности.
- Организация проведения аудита информационной безопасности.
- Основные этапы проведения аудита информационной безопасности.
- Менеджмент аудита информационной безопасности (провести анализ мероприятий этапов менеджмента).
- Подготовка к проведению аудита информационной безопасности на месте (провести анализ проводимых мероприятий).
- Проведение аудита информационной безопасности на месте (провести анализ про-водимых мероприятий).
- Подготовка и рассылка отчета по аудиту информационной безопасности (раскрыть особенности составления и содержания отчета).
- Разработка плана аудита ИБ для коммерческого банка (PCI DSS).
- Разработка плана аудита ИБ для коммерческого банка (ГОСТ Р 57580.1-2017).
- Разработка плана аудита ИБ для коммерческого банка (Непрерывность бизнеса).
- Разработка плана аудита ИБ для коммерческого банка (Тест на проникновение).
- Особенности проведения аудита персональных данных (в соответствии с ПП-1119).

График выполнения курсового проекта

Неделя	1 - 4	5 - 8	9 - 12	13 - 16	Зачетная
Раздел курсового	1	2, 3	2, 3	4	Защита курсового

проекта					проекта
Объем раздела, %	25	25	25	25	-
Выполненный объем нарастающим итогом, %	25	50	75	100	-

Номер раздела	Раздел курсового проекта
1	Р1. Задание на курсовую работу. Введение курсовой работы
2	Р2. Первая глава основной части курсовой работы
3	Р3. Вторая глава основной части курсовой работы
4	Р4. Заключение. Список использованных источников

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:					
–требования нормативных и правовых документов (законы, стандарты, регламенты) в предметной области дисциплины;	ИД-3$_{РПК-1}$	+	+		Тестирование/Тест № 1
–основы менеджмента безопасности информационных систем;	ИД-3$_{РПК-1}$		+		Контрольная работа/Контрольная работа № 1
–основы аудита безопасности информационных систем;	ИД-4$_{РПК-1}$			+	Тестирование/Тест № 2
–особенности практической организации и проведения аудита безопасности информационных систем.	ИД-4$_{РПК-1}$			+	Контрольная работа/Контрольная работа № 2
Уметь:					
–разрабатывать и управлять программой аудита безопасности информационных систем;	ИД-3$_{РПК-1}$		+		Коллоквиум/Коллоквиум № 1
–проводить мероприятия по управлению программой безопасности информационных систем;	ИД-3$_{РПК-1}$		+		Коллоквиум/Коллоквиум № 1
–проводить основные организационные мероприятия по проведению аудита безопасности информационных систем;	ИД-4$_{РПК-1}$			+	Коллоквиум/Коллоквиум № 2
–оформлять необходимые документы в рамках аудита безопасности информационных систем.	ИД-4$_{РПК-1}$			+	Коллоквиум/Коллоквиум № 4
–осуществлять оценку соответствия информационной безопасности предприятия;	ИД-4$_{РПК-1}$			+	Коллоквиум/Коллоквиум № 3

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

4.1. Текущий контроль успеваемости

9 семестр

Форма реализации: Компьютерное задание

1. Контрольная работа № 2 (Контрольная работа)

Форма реализации: Письменная работа

1. Коллоквиум № 1 (Коллоквиум)
2. Коллоквиум № 2 (Коллоквиум)
3. Коллоквиум № 3 (Коллоквиум)
4. Коллоквиум № 4 (Коллоквиум)
5. Контрольная работа № 1 (Контрольная работа)
6. Тест № 1 (Тестирование)
7. Тест № 2 (Тестирование)

Балльно-рейтинговая структура дисциплины является приложением А.
Балльно-рейтинговая структура курсовой работы является приложением Б.

4.2 Промежуточная аттестация по дисциплине

Экзамен (Семестр №9)

Итоговая оценка выставляется по итогам экзамена, с учетом оценки за курсовую работу и оценок по текущей успеваемости.

Курсовая работа (КР) (Семестр №9)

Итоговая оценка выставляется по итогам экзамена, с учетом оценки за курсовую работу и оценок по текущей успеваемости.

В диплом выставляется оценка за 9 семестр.

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

5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1 Печатные и электронные издания:

1. "Broadcasting: телевидение и радиовещание", Издательство: "ГРОТЕК", Москва, 2013 - (55 с.)
https://biblioclub.ru/index.php?page=book&id=210605;
2. Правовое обеспечение контроля, учета, аудита и судебно-экономической экспертизы : учебник для студентов вузов, обучающихся по юридическим, экономическим направлениям / Е. М. Ашмарина, Н. М. Артемов, А. Б. Быля, [и др.] ; ред. Е. М. Ашмарина. – 2-е изд., перераб. и доп. – Москва : Юрайт, 2020. – 299 с. – (Высшее образование). – Под общим руководством В. В. Ершова. – ISBN 978-5-534-09038-3.;
3. 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.;

4. Организационно-правовое обеспечение информационной безопасности : учебное пособие для вузов по специальностям 090102 "Компьютерная безопасность", 090105 "Комплексное обеспечение информационной безопасности автоматизированных систем", 090106 "Информационная безопасность телекоммуникационных систем" / А. А. Стрельцов, [и др.]. – М. : АКАДЕМИЯ, 2008. – 256 с. – (Высшее профессиональное образование). – ISBN 978-5-7695-4240-4.;
5. Анисимов, А. А. Менеджмент в сфере информационной безопасности : учебное пособие / А. А. Анисимов. – М. : БИНОМ. Лаборатория знаний : Интернет-Ун-т информ. технологий, 2010. – 176 с. – (Основы информационных технологий). – ISBN 978-5-9963-0237-6..

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

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. **Электронные ресурсы издательства Springer** - https://link.springer.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. **Журнал Science** - https://www.sciencemag.org/
9. **Журналы издательства Wiley** - https://onlinelibrary.wiley.com/
10. **Электронная библиотека МЭИ (ЭБ МЭИ)** - http://elib.mpei.ru/login.php
11. **Информационно-справочная система «Кодекс/Техэксперт»** - Http:\\proinfosoft.ru; http://docs.cntd.ru/

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Тип помещения	Номер аудитории, наименование	Оснащение
Учебные аудитории для проведения лекционных занятий и текущего контроля	К-601, Учебная аудитория	парта со скамьей, стол преподавателя, стул, трибуна, доска меловая, мультимедийный проектор, экран
	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
Учебные аудитории для проведения практических занятий, КР и КП	М-510, Учебная лаборатория информационно-аналитический технологий - компьютерный класс	стул, стол письменный, мультимедийный проектор, экран, доска маркерная, компьютер персональный, кондиционер
Учебные аудитории для	М-510, Учебная	стул, стол письменный,

проведения промежуточной аттестации	лаборатория информационно-аналитический технологий - компьютерный класс	мультимедийный проектор, экран, доска маркерная, компьютер персональный, кондиционер
	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
Помещения для самостоятельной работы	НТБ-303, Лекционная аудитория	стол компьютерный, стул, стол письменный, вешалка для одежды, компьютерная сеть с выходом в Интернет, компьютер персональный, принтер, кондиционер
Помещения для консультирования	А-317, Учебная аудитория	парта со скамьей, стол преподавателя, 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

Аудит безопасности информационных систем

(название дисциплины)

9 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:

КМ-1 Тест № 1 (Тестирование)
КМ-1 Контрольная работа № 1 (Контрольная работа)
КМ-2 Тест № 2 (Тестирование)
КМ-2 Контрольная работа № 2 (Контрольная работа)
КМ-3 Коллоквиум № 2 (Коллоквиум)
КМ-3 Коллоквиум № 1 (Коллоквиум)
КМ-4 Коллоквиум № 3 (Коллоквиум)
КМ-4 Коллоквиум № 4 (Коллоквиум)

Вид промежуточной аттестации – Экзамен.

Номер раздела	Раздел дисциплины	Индекс КМ:	КМ-1	КМ-1	КМ-2	КМ-2	КМ-3	КМ-3	КМ-4	КМ-4
		Неделя КМ:	4	4	8	8	12	12	15	15
1	Вводная лекция									
1.1	Понятие и виды аудита информационной безопасности		+							
2	Менеджмент аудита безопасности информационных систем									
2.1	Правовые основы аудита информационной безопасности		+					+		
2.2	Способы и цели контроля и проверки процессов и систем			+				+		
2.3	Виды аудита информационной безопасности			+				+		
2.4	Менеджмент аудита информационной безопасности			+				+		
2.5	Программа аудита информационной безопасности			+				+		
3	Особенности проведения аудита безопасности информационных систем									
3.1	Основные этапы аудита информационной безопасности				+	+				
3.2	Проведение аудита информационной безопасности					+				
3.3	Способы оценки информационной безопасности				+	+	+			

3.4	Модели оценки информационной безопасности			+					+
3.5	Аудит управления непрерывностью бизнеса				+				+
3.6	Проведение аудита информационной безопасности в организациях банковской системы России			+	+				
3.7	Проведение категорирования и аудита информационной безопасности объектов критической информационной инфраструктуры			+				+	
	Вес КМ, %:	10	15	10	15	15	10	10	15

Приложение Б

БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА КУРСОВОГО ПРОЕКТА/РАБОТЫ ПО ДИСЦИПЛИНЕ

Аудит безопасности информационных систем

(название дисциплины)

9 семестр

Перечень контрольных мероприятий <u>текущего контроля</u> успеваемости по курсовой работе:

КМ-1 КМ-1Соблюдение графика выполнения КР
КМ-2 КМ-2Оценка выполнения разделов КР
КМ-3 КМ-3 Качество оформления КР
КМ-4 КМ-4Качество содержания КР

Вид промежуточной аттестации – защита КР.

Номер раздела	Раздел курсового проекта/курсовой работы	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
		Неделя КМ:	4	8	12	16
1	Р1. Задание на курсовую работу. Введение курсовой работы		+			
2	Р2. Первая глава основной части курсовой работы			+	+	
3	Р3. Вторая глава основной части курсовой работы			+	+	
4	Р4. Заключение. Список использованных источников					+
		Вес КМ, %:	25	25	25	25