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: Организация и технология защиты информации

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очная

Рабочая программа дисциплины
АУДИТ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Блок:	**Блок 1 «Дисциплины (модули)»**
Часть образовательной программы:	**Вариативная**
№ дисциплины по учебному плану:	**Б1.В.05**
Трудоемкость в зачетных единицах:	**7 семестр - 6;**
Часов (всего) по учебному плану:	**216 часов**
Лекции	**7 семестр - 32 часа;**
Практические занятия	**7 семестр - 32 часа;**
Лабораторные работы	**не предусмотрено учебным планом**
Консультации	**7 семестр - 18 часов;**
Самостоятельная работа	**7 семестр - 129,2 часа;**
в том числе на КП/КР	**7 семестр - 95,7 часа;**
Иная контактная работа	**7 семестр - 4 часа;**
включая: **Тестирование** **Контрольная работа**	
Промежуточная аттестация:	
Защита курсовой работы **Экзамен**	**7 семестр - 0,3 часа;** **7 семестр - 0,5 часа;** **всего - 0,8 часа**

Москва 2020

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 организации 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
ОПК-7 способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты		знать: - требования нормативных и правовых документов (законы, стандарты, регламенты) в предметной области дисциплины;. уметь: - определять виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия;.
ПК-10 способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности		знать: - требования стандартов. уметь: - участвовать в работах по реализации политики информационной безопасности;; - проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов, разрабатывать предложения по совершенствованию системы управления информационной безопасностью;.
ПК-12 способностью принимать участие в проведении экспериментальных исследований системы		знать: - направления и перспективы дальнейшего совершенствования систем обеспечения безопасности хозяйствующих субъектов;.

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Запланированные результаты обучения
защиты информации		уметь: - проводить экспериментальные исследования системы защиты информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к части, формируемой участниками образовательных отношений блока дисциплин основной профессиональной образовательной программе Организация и технология защиты информации (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	20	7	10	-	10	-	-	-	-	-	-	-	***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Вводная лекция" ***Изучение материалов литературных источников:*** [1], 1-416 [4], 1-299 [5], 1-55
1.1	Вводная лекция	20		10	-	10	-	-	-	-	-	-	-	
2	Менеджмент аудита безопасности информационных систем	20		10	-	10	-	-	-	-	-	-	-	***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы ***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: ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "2. Менеджмент аудита безопасности
2.1	Тема 1. Понятие и виды аудита безопасности информационных систем	4		2	-	2	-	-	-	-	-	-	-	
2.2	Тема 2. Стандарты аудита безопасности информационных систем.	12		6	-	6	-	-	-	-	-	-	-	
2.3	Тема 3. Менеджмент аудита безопасности информационных	4		2	-	2	-	-	-	-	-	-	-	

	систем.													информационных систем" ***<u>Подготовка к практическим занятиям:</u>*** Изучение материала по разделу "2. Менеджмент аудита безопасности информационных систем" подготовка к выполнению заданий на практических занятиях ***<u>Подготовка к контрольной работе:</u>*** Изучение материалов по разделу 2. Менеджмент аудита безопасности информационных систем и подготовка к контрольной работе ***<u>Подготовка домашнего задания:</u>*** Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "2. 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. ***<u>Подготовка к текущему контролю:</u>*** Повторение материала по разделу "2. Менеджмент аудита безопасности информационных систем" ***<u>Изучение материалов литературных источников:</u>*** [1], 1-416 [3], 1-176
3	Особенности проведения аудита безопасности информационных систем	24		12	-	12	-	-	-	-	-	-	-	***<u>Подготовка к текущему контролю:</u>*** Повторение материала по разделу "3. Особенности проведения аудита безопасности информационных систем" ***<u>Подготовка к аудиторным занятиям:</u>***
3.1	Тема 4. Основные этапы аудита	4		2	-	2	-	-	-	-	-	-	-	Проработка лекции, выполнение и подготовка к защите лаб. работы

	безопасности информационных систем													***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "3. Особенности проведения аудита безопасности информационных систем" ***Подготовка к практическим занятиям:*** Изучение материала по разделу "3. Особенности проведения аудита безопасности информационных систем" подготовка к выполнению заданий на практических занятиях ***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 контрольной работе:*** Изучение материалов по разделу 3. Особенности проведения аудита безопасности информационных систем и подготовка к контрольной работе ***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 домашнего задания:*** Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "3. Особенности проведения аудита безопасности информационных систем" материалу. Дополнительно студенту необходимо изучить литературу и разобрать
3.2	Тема 5. Методы оценивания информационной безопасности	4		2	-	2	-	-	-	-	-	-	-	
3.3	Тема 6. Аудит управления непрерывностью бизнеса и восстановления после сбоев	8		4	-	4	-	-	-	-	-	-	-	
3.4	Тема 7. Активный аудит информационной безопасности	8		4	-	4	-	-	-	-	-	-	-	

														примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам. ***Изучение материалов литературных источников:*** [2], 1-256
	Экзамен	36.0		-	-	-	-	2	-	-	0.5	-	33.5	
	Курсовая работа (КР)	116.0		-	-	-	16	-	4	-	0.3	95.7	-	
	Всего за семестр	**216.0**		**32**	**-**	**32**	**16**	**2**	**4**	**-**	**0.8**	**95.7**	**33.5**	
	Итого за семестр	**216.0**		**32**	**-**	**32**	**18**		**4**		**0.8**	**129.2**		

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. Вводная лекция

Предмет и задачи курса. Значение и место курса в подготовке специалистов по защите информации. Взаимосвязь курса с другими дисциплинами. Роль и место аудита безопасности информационных систем в обеспечении информационной безопасности хозяйствующего субъекта. Разделы и темы, их распределение по видам аудиторных занятий. Формы проведения семинарских занятий..

2. Менеджмент аудита безопасности информационных систем

2.1. Тема 1. Понятие и виды аудита безопасности информационных систем

Аудит безопасности информационных систем (оценка соответствия требованиям информационной безопасности): сущность аудита, понятие аудита, основные виды аудита. Необходимость в проведении аудита безопасности информационных систем. Периодичность проведения аудита безопасности информационных систем Международные стандарты в области информационной безопасности и лучшие практики по оценке соответствия безопасности информационных систем. Цели и задачи аудита безопасности информационных систем. Основные принципы аудита безопасности информационных систем..

2.2. Тема 2. Стандарты аудита безопасности информационных систем.

Основные стандарты в области управления информационной безопасностью и информационных технологий об оценке качества информационных систем и их соответствия требованиям информационной безопасности. Подходы к стандартизации области оценки информационной безопасности в стандартах серии ISO 270xx, 15408, COBIT, ITIL. Международный стандарт ISO 19011..

2.3. Тема 3. Менеджмент аудита безопасности информационных систем.

Понятие менеджмента аудита безопасности информационных систем. Процессная модель аудита безопасности информационных систем. Этапы менеджмента аудита. Подготовка и планирование системы менеджмента. Использование системы менеджмента. Анализ и совершенствование системы менеджмента аудита безопасности информационных систем. План и программа аудита безопасности информационных систем. Разработка, управление и совершенствование программы аудита. Формирование группы аудита безопасности информационных систем, распределение ролей в группе..

3. Особенности проведения аудита безопасности информационных систем

3.1. Тема 4. Основные этапы аудита безопасности информационных систем

Основные этапы проведения аудита безопасности информационных систем: инициирование процедуры аудита, сбор информации аудита, анализ данных аудита, выработка рекомендаций, подготовка аудиторского отчета. Состав и порядок работ по каждому этапу. Порядок и формы получения свидетельств аудита безопасности информационных систем. Основные подходы к оценке полученных свидетельств аудита..

3.2. Тема 5. Методы оценивания информационной безопасности

Оценивание информационной безопасности на основе показателей информационной безопасности. Модель оценки информационной безопасности. Основные элементы процесса проведения аудита безопасности информационных систем. Шкала оценивания процессов

обеспечения информационной безопасности. Метрики оценки состояния информационной безопасности. Подход на примере формирования метрик в соответствии со стандартом NIST Special Publication 800-55 Security Metrics Guide for Information Technology Systems. Особенности формирования частных, обобщенных и комплексных показателей информационной безопасности..

3.3. Тема 6. Аудит управления непрерывностью бизнеса и восстановления после сбоев

Методологии, стандарты и нормативные требования в области управления непрерывностью бизнеса. Основные направления оценки в области управления непрерывностью бизнеса. Процедуры резервирования оборудования. Процедуры резервного копирования и восстановления данных. Понятие катастрофоустойчивой модели бизнеса, основные направления ее реализации. План восстановления после прерывания бизнеса..

3.4. Тема 7. Активный аудит информационной безопасности

Понятие активного аудита информационной безопасности. Виды активного аудита. Методологии, стандарты и нормативные требования в области активного аудита информационной безопасности. Сканирование информационных ресурсов. Виды уязвимостей. Порядок обработки выявленных уязвимостей. Используемое ПО сканирования. Тесты на проникновение. Виды тестов и особенности их проведения. Порядок тестирования и использования полученных результатов. Используемое ПО для тестирования..

3.3. Темы практических занятий

1. 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»;
2. 8.Использование специализированного программного обеспечения аудита информационной безопасности на примере ПО Estimate Tools;
3. 7.Отчетность по аудиту безопасности информационных систем. Подготовка отчета и заключения по аудиту;
4. 6.Сканирование на уязвимости, тесты на проникновение. Особенности проведения и использования полученных результатов;
5. 5.Активный аудит информационной безопасности: виды, методы, используемые средства;
6. 4.Особенности проведения работ в ходе аудита безопасности информационных систем;
7. 3.План и программа аудита безопасности информационных систем. Менеджмент программа аудита;
8. 1.Способы контроля и проверки процес1.Способы контроля и проверки процессов информационных систем. Цели контроля и проверки процессов и системсов 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 "3. Особенности проведения аудита безопасности информационных систем"

Групповые консультации по разделам дисциплины (ГК)

1. Обсуждение материалов по кейсам раздела "Вводная лекция"
2. Обсуждение материалов по кейсам раздела "Менеджмент аудита безопасности информационных систем"
3. Обсуждение материалов по кейсам раздела "3. 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 "3. 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 "3. Особенности проведения аудита безопасности информационных систем"

3.6 Тематика курсовых проектов/курсовых работ

7 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.
- 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.
- 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.

График выполнения курсового проекта

Неделя	1 - 4	5 - 8	9 - 12	13 - 15	Зачетная
Раздел курсового проекта	1	2, 3	2, 3	4	Защита курсового проекта
Объем раздела, %	25	25	25	25	-
Выполненный объем нарастающим итогом, %	25	50	75	100	-

Номер раздела	Раздел курсового проекта
1	Задание на курсовую работу. Введение курсовой работы
2	Первая глава основной части курсовой работы
3	Вторая глава основной части курсовой работы
4	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;	ОПК-7(Компетенция)	+			Контрольная работа/Практическое задание № 1. Требования национальных и международных нормативных актов, предписывающих и регламентирующих проведение инструментального контроля в коммерческом банке
требования стандартов	ПК-10(Компетенция)		+		Контрольная работа/Практическое задание № 2-3. Планирование аудита информационной безопасности, с использованием различных стандартов информационной безопасности (СТО БР ИББС 1.2-2014, ГОСТ 57580.2-2018, Положение № 382-П, ГОСТ 27001, PCI DSS и т.п.);
направления и перспективы дальнейшего совершенствования систем обеспечения безопасности хозяйствующих субъектов;	ПК-12(Компетенция)	+			Тестирование/Система менеджмента аудита безопасности информационных систем
Уметь:					
определять виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия;	ОПК-7(Компетенция)			+	Контрольная работа/Практическое задание № 4. Разработка отчета и заключения по аудиту информационной безопасности аттестуемого объекта
проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов, разрабатывать предложения по	ПК-10(Компетенция)			+	Контрольная работа/Практическое задание № 4. Разработка отчета и заключения по аудиту информационной безопасности аттестуемого объекта

совершенствованию системы управления информационной безопасностью;					
участвовать в работах по реализации политики информационной безопасности;	ПК-10(Компетенция)		+		Контрольная работа/Практическое задание № 2-3. Планирование аудита информационной безопасности, с использованием различных стандартов информационной безопасности (СТО БР ИББС 1.2-2014, ГОСТ 57580.2-2018, Положение № 382-П, ГОСТ 27001, PCI DSS и т.п.);
проводить экспериментальные исследования системы защиты информации	ПК-12(Компетенция)			+	Контрольная работа/Практическое задание № 2-3. Планирование аудита информационной безопасности, с использованием различных стандартов информационной безопасности (СТО БР ИББС 1.2-2014, ГОСТ 57580.2-2018, Положение № 382-П, ГОСТ 27001, PCI DSS и т.п.);

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: Письменная работа

1. Практическое задание № 1. Требования национальных и международных нормативных актов, предписывающих и регламентирующих проведение инструментального контроля в коммерческом банке (Контрольная работа)
2. Практическое задание № 2-3. Планирование аудита информационной безопасности, с использованием различных стандартов информационной безопасности (СТО БР ИББС 1.2-2014, ГОСТ 57580.2-2018, Положение № 382-П, ГОСТ 27001, PCI DSS и т.п.); (Контрольная работа)
3. Практическое задание № 4. Разработка отчета и заключения по аудиту информационной безопасности аттестуемого объекта (Контрольная работа)
4. Система менеджмента аудита безопасности информационных систем (Тестирование)

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

4.2 Промежуточная аттестация по дисциплине

Экзамен (Семестр №7)

Оценка выставляется как среднее арифметическое - оценка по курсу и оценка за экзамен.

Курсовая работа (КР) (Семестр №7)

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

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. 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. 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 .;
3. 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 .;

4. 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 .;
5. "Broadcasting: телевидение и радиовещание", Издательство: "ГРОТЕК", Москва, 2013 - (55 с.)
https://biblioclub.ru/index.php?page=book&id=210606.

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. **Электронные ресурсы издательства Springer** - https://link.springer.com/
5. **База данных Web of Science** - http://webofscience.com/
6. **База данных Scopus** - http://www.scopus.com
7. **Журнал Science** - https://www.sciencemag.org/
8. **Электронная библиотека МЭИ (ЭБ МЭИ)** - http://elib.mpei.ru/login.php
9. **Информационно-справочная система «Кодекс/Техэксперт»** - Http:\\proinfosoft.ru; http://docs.cntd.ru/
10. **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	З-512, Учебная аудитория	парта, стол преподавателя, стул, доска меловая
Учебные аудитории для проведения промежуточной аттестации	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
	З-512, Учебная аудитория	парта, стол преподавателя, стул, доска меловая
Помещения для самостоятельной	НТБ-303, Компьютерный	стол компьютерный, стул, стол письменный, вешалка для одежды,

работы	читальный зал	компьютерная сеть с выходом в Интернет, компьютер персональный, принтер, кондиционер
	К-307, Учебная лаборатория "Открытое программное обеспечение"	стол преподавателя, стол компьютерный, стол учебный, стул, вешалка для одежды, тумба, компьютерная сеть с выходом в Интернет, мультимедийный проектор, экран, доска маркерная, сервер, компьютер персональный, кондиционер
	К-302, Учебная лаборатория "Информационно-аналитические технологии"	стол преподавателя, стол компьютерный, стул, мультимедийный проектор, экран, доска маркерная, сервер, компьютер персональный, кондиционер
Помещения для консультирования	З-512, Учебная аудитория	парта, 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)

7 семестр

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

КМ-1 Система менеджмента аудита безопасности информационных систем (Тестирование)

КМ-2 Практическое задание № 1. Требования национальных и международных нормативных актов, предписывающих и регламентирующих проведение инструментального контроля в коммерческом банке (Контрольная работа)

КМ-3 Практическое задание № 2-3. Планирование аудита информационной безопасности, с использованием различных стандартов информационной безопасности (СТО БР ИББС 1.2-2014, ГОСТ 57580.2-2018, Положение № 382-П, ГОСТ 27001, PCI DSS и т.п.); (Контрольная работа)

КМ-4 Практическое задание № 4. Разработка отчета и заключения по аудиту информационной безопасности аттестуемого объекта (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	Вводная лекция					
1.1	Вводная лекция		+	+		
2	Менеджмент аудита безопасности информационных систем					
2.1	Тема 1. Понятие и виды аудита безопасности информационных систем				+	
2.2	Тема 2. Стандарты аудита безопасности информационных систем.				+	
2.3	Тема 3. Менеджмент аудита безопасности информационных систем.				+	
3	Особенности проведения аудита безопасности информационных систем					
3.1	Тема 4. Основные этапы аудита безопасности информационных систем				+	+
3.2	Тема 5. Методы оценивания информационной безопасности				+	+
3.3	Тема 6. Аудит управления непрерывностью бизнеса и восстановления после сбоев				+	+
3.4	Тема 7. Активный аудит информационной безопасности				+	+
		Вес КМ, %:	25	25	25	25

Приложение Б

БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА КУРСОВОГО ПРОЕКТА/РАБОТЫ ПО ДИСЦИПЛИНЕ

Аудит безопасности информационных систем

(название дисциплины)

7 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по курсовой работе:

КМ-1 Соблюдение графика выполнения КР
КМ-2 Оценка выполнения разделов КР
КМ-3 Качество оформления КР
КМ-4 Качество 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	15
1	Задание на курсовую работу. Введение курсовой работы		+			
2	Первая глава основной части курсовой работы			+	+	
3	Вторая глава основной части курсовой работы			+	+	
4	Заключение. Список использованных источников					+
		Вес КМ, %:	25	25	25	25