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

Оценочные материалы
по дисциплине
Аудит безопасности информационных систем

Москва
2023

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Разработчик	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

ОБЩАЯ ЧАСТЬ

Оценочные материалы по дисциплине предназначены для оценки: достижения обучающимися запланированных результатов обучения по дисциплине, этапа формирования запланированных компетенций и уровня освоения дисциплины.

Оценочные материалы по дисциплине включают оценочные средства для проведения мероприятий текущего контроля успеваемости и промежуточной аттестации.

Формируемые у обучающегося компетенции:

1. 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

2. ПК-10 способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности

3. ПК-12 способностью принимать участие в проведении экспериментальных исследований системы защиты информации

и включает:

для текущего контроля успеваемости:

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)

БРС дисциплины

7 семестр

Раздел дисциплины	Веса контрольных мероприятий, %				
	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
	Срок КМ:	4	8	12	15
Вводная лекция					
Вводная лекция		+	+		

Менеджмент аудита безопасности информационных систем				
Тема 1. Понятие и виды аудита безопасности информационных систем			+	
Тема 2. Стандарты аудита безопасности информационных систем.			+	
Тема 3. Менеджмент аудита безопасности информационных систем.			+	
Особенности проведения аудита безопасности информационных систем				
Тема 4. Основные этапы аудита безопасности информационных систем			+	+
Тема 5. Методы оценивания информационной безопасности			+	+
Тема 6. Аудит управления непрерывностью бизнеса и восстановления после сбоев			+	+
Тема 7. Активный аудит информационной безопасности			+	+
Вес КМ:	25	25	25	25

$Общая часть/Для промежуточной аттестации$

БРС курсовой работы/проекта

7 семестр

Раздел дисциплины	Веса контрольных мероприятий, %				
	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
	Срок КМ:	4	8	12	15
Задание на курсовую работу. Введение курсовой работы		+			
Первая глава основной части курсовой работы			+	+	
Вторая глава основной части курсовой работы			+	+	
Заключение. Список использованных источников					+
Вес КМ:		25	25	25	25

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ТЕКУЩЕГО КОНТРОЛЯ

I. Оценочные средства для оценки запланированных результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Индекс компетенции	Индикатор	Запланированные результаты обучения по дисциплине	Контрольная точка
ОПК-7	ОПК-7(Компетенция)	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;	Практическое задание № 1. Требования национальных и международных нормативных актов, предписывающих и регламентирующих проведение инструментального контроля в коммерческом банке (Контрольная работа) Практическое задание № 4. Разработка отчета и заключения по аудиту информационной безопасности аттестуемого объекта (Контрольная работа)
ПК-10	ПК-10(Компетенция)	Знать: требования стандартов Уметь: участвовать в работах по реализации политики информационной безопасности;	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) Практическое задание № 4. Разработка отчета и заключения по аудиту информационной безопасности аттестуемого объекта (Контрольная

		проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов, разрабатывать предложения по совершенствованию системы управления информационной безопасностью;	работа)
ПК-12	ПК-12(Компетенция)	Знать: направления и перспективы дальнейшего совершенствования систем обеспечения безопасности хозяйствующих субъектов; Уметь: проводить экспериментальные исследования системы защиты информации	Система менеджмента аудита безопасности информационных систем (Тестирование) 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)

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. Система менеджмента аудита безопасности информационных систем

Формы реализации: Письменная работа
Тип контрольного мероприятия: Тестирование
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Студенты отвечают письменно на заданные вопросы.

Краткое содержание задания:
Выполняется письменная работа

Контрольные вопросы/задания:

Знать: направления и перспективы дальнейшего совершенствования систем обеспечения безопасности хозяйствующих субъектов;	1.*Какие методологические подходы к решению проблемы доверия к мерам ИБ используются в настоящее время?*

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

Оценка: 2
Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

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

Формы реализации: Письменная работа
Тип контрольного мероприятия: Контрольная работа
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Студенты отвечают письменно на заданные вопросы.

Краткое содержание задания:

Выполняется письменная работа

Контрольные вопросы/задания:

Знать: требования нормативных и правовых документов (законы, стандарты, регламенты) в предметной области дисциплины;	1.*Риски программы аудита информационной безопасности.*

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

Оценка: 2
Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

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.);

Формы реализации: Письменная работа
Тип контрольного мероприятия: Контрольная работа
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Студенты отвечают письменно на заданные вопросы.

Краткое содержание задания:
Выполняется письменная работа

Контрольные вопросы/задания:

Знать: требования стандартов	1.*Основные этапы проведения аудита безопасности информационных систем.* 2.*Порядок и формы получения свидетельств аудита безопасности информационных систем.* 3.*Формирование группы аудита безопасности информационных систем, распределение ролей в группе.*
Уметь: участвовать в работах по реализации политики	1.*Основные подходы к оценке полученных свидетельств аудита.*

информационной безопасности;	
Уметь: проводить экспериментальные исследования системы защиты информации	1.*Документация системы менеджмента аудита безопасности информационных систем.* 2.*Отчет и заключение по аудиторской проверке.*

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

Оценка: 2
Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

КМ-4. Практическое задание № 4. Разработка отчета и заключения по аудиту информационной безопасности аттестуемого объекта

Формы реализации: Письменная работа
Тип контрольного мероприятия: Контрольная работа
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Студенты отвечают письменно на заданные вопросы.

Краткое содержание задания:
Студенты отвечают письменно на заданные вопросы.

Контрольные вопросы/задания:

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;	1.определить порядок рассылки и хранения отчета по аудиту информационной безопасности.
Уметь: проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов, разрабатывать предложения по	1.оформить отчет по аудиту информационной безопасности по результатам, полученным в ходе оценки

совершенствованию системы управления информационной безопасностью;	

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

Оценка: 2
Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

7 семестр

Форма промежуточной аттестации: Экзамен

Пример билета

<table>
<tr><td rowspan="4">М Э И</td><td>ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № “Инженерно-экономический институт” МЭИ (ТУ)</td><td>3</td><td>Утверждаю

2019 г.</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td>Дисциплина</td><td colspan="2">Аудит безопасности информационных систем</td></tr>
<tr><td>Преподаватель</td><td colspan="2">К.т.н., доцент Писаренко И.В.</td></tr>
<tr><td colspan="4">1. Основные стандарты в области аудита безопасности информационных систем. Содержание (кратко) и область действия стандартов.
2. Порядок формирования группы по аудиту информационной безопасности. Компетентность и оценка аудиторов.</td></tr>
</table>

Процедура проведения

Экзамен проводится по билетам, в письменной форме. Время написания ответа - 20-25 минут.

I. Перечень компетенций/индикаторов и контрольных вопросов проверки результатов освоения дисциплины

1. Компетенция/Индикатор: ОПК-7(Компетенция)

Вопросы, задания

1.Принципы аудита безопасности информационных систем. Дать комментарии по каждому принципу.
2.Виды аудита безопасности информационных систем. Цели и решаемые задачи по каждому виду аудита.
3.Комплексный аудит безопасности информационных систем. Цели, решаемые задачи. Особенности проведения.
4.Активный аудит информационной безопасности. Разновидности аудита, решаемые задачи.
5.Процесс оценивания. Схема процесса оценивания. Основные элементы процесса оценивания.
6.Входные и выходные данные оценки безопасности информационных систем. Привести примеры.
7.Планирование программы аудита информационной безопасности. Особенности планирования. Ресурсы программы аудита.
8.Осознание аудита информационной безопасности. Цели, входные и выходные данные. Основные мероприятия.
9. Основные этапы проведения аудита информационной безопасности.
10.Организация проведения аудита информационной безопасности.

Материалы для проверки остаточных знаний

1.Проведение аудита информационной безопасности на месте. Сбор и анализ исходных данных при проведении аудита.

Ответы:

Ответ дается в письменной форме, возможны уточняющие вопросы преподавателя.

Верный ответ: Процесс сбора информации аудита ИБ является наиболее сложным и длительным. Это связано в основном с большими объемами работ, возможным отсутствием необходимой документации на информационные системы и с необходимостью плотного взаимодействия аудитора со многими должностными лицами организации. На данном этапе проводятся сбор исходных данных от заказчика, их предварительный анализ, а также организационные мероприятия по подготовке проведения аудита. На этом этапе собирается информация и дается оценка следующих мер и средств: •Организационных мер в области ИБ; •Программно-технических средств защиты информации; •Обеспечения физической безопасности. Анализируются следующие характеристики построения и функционирования корпоративной информационной системы: •Организационные характеристики; •Организационно-технические характеристики; •Технические характеристики, связанные с архитектурой ИС; •Технические характеристики, связанные с конфигурацией сетевых устройств и серверов ИС; •Технические характеристики, связанные с использованием встроенных механизмов ИБ.

2. Компетенция/Индикатор: ПК-10(Компетенция)

Вопросы, задания

1.Понятие аудита. Понятия «Аудит безопасности информационных систем» и «Аудит информационной безопасности». Область каждого из аудитов, цели, решаемые задачи.
2.Основные стандарты в области аудита безопасности информационных систем. Содержание (кратко) и область действия стандартов.
3.Требования законодательства Российской Федерации и нормативных документов регулирующих органов по проведению аудита (оценки соответствия) в области информационной безопасности.
4.Необходимость в проведении аудита безопасности информационных систем. Дать комментарии, привести примеры.
5.Основные способы аудита безопасности информационных систем. Дать комментарии, привести примеры.
6.Роли и обязанности ответственных лиц по проведению оценки соответствия.
7.Цели и объем программы аудита информационной безопасности. Риски программы информационной безопасности.
8.Компетентность лица, ответственного за управление программой аудита информационной безопасности.

Материалы для проверки остаточных знаний

1.Аудит управления непрерывностью бизнеса и восстановления после сбоев.

Ответы:

Ответ дается в письменной форме, возможны уточняющие вопросы преподавателя.

Верный ответ: Основной целью аудита управления (обеспечения) непрерывностью бизнеса и восстановления после сбоев является необходимость убедиться в том, что в организации внедрены контрольные механизмы, минимизирующие риски прерываний критичных бизнес-процессов и негативные последствия таких прерываний, в частности: •проведена оценка рисков прерываний, и разработан план действий по внедрению корректирующих мер контроля, и на данные меры выделены соответствующие бюджеты; •данный план действий выполняется и контролируется руководством; •соответствующие политики, стандарты, процедуры в области

обеспечения непрерывности и соответствующие договорные соглашения исполняются, как это установлено; •ИТ-системы, данные и другие ресурсы, необходимые для восстановления, будут доступны в соответствии с установленными требованиями; •план непрерывности бизнеса и восстановления ИТ после сбоев разработан, адекватен и соответствует текущим потребностям организации; •разработаны и внедрены процедуры обеспечения безопасности персонала в критичных ситуациях. Основные вопросы, рассматриваемые при аудите В ходе аудита обычно рассматриваются следующие аспекты управления непрерывностью бизнеса: •политики и основы процессов управления непрерывностью бизнеса; •процедуры действий в чрезвычайных ситуациях; •оценка рисков и анализ влияния прерываний на бизнес, управление рисками; •компоненты планирования непрерывности бизнеса; •стратегии обеспечения непрерывности бизнеса и восстановления после сбоев; •ресурсы, требуемые для восстановления; •разработка и внедрение планов непрерывности бизнеса и восстановления ИТ после сбоев; •процедуры альтернативной работы подразделений; •удаленное хранение резервной информации; •резервная площадка; •распространение планов; •обучение, тренировки; •тестирование, поддержка и пересмотр планов; •заключительные процедуры.

3. Компетенция/Индикатор: ПК-12(Компетенция)

Вопросы, задания

1.Концептуальная схема аудита безопасности информационных систем. Рассмотреть типовые случаи целесообразности проведения аудита.

2.Программа аудита информационной безопасности. Содержание программы. Управление программой аудита.

3.Внедрение программы аудита информационной безопасности: перечислить задачи, дать комментарии по каждой задаче.

4.Первоначальный контакт аудиторской организации с проверяемой организацией. Цели и задачи первоначального контакта.

5.Завершение аудита информационной безопасности. Вопросы, решаемые в ходе заключительного совещания.

6.Оценивание информационной безопасности на основе показателей информационной безопасности.

7.Аудит управления непрерывностью бизнеса и восстановления после сбоев.

Материалы для проверки остаточных знаний

1.Первоначальный контакт аудиторской организации с проверяемой организацией. Цели и задачи первоначального контакта.

Ответы:

Ответ дается в письменной форме, возможны уточняющие вопросы преподавателя.

Верный ответ: Первоначальный контакт с проверяемой организацией для проведения аудита ИБ может иметь официальный или неформальный характер и должен устанавливаться с руководителем группы по аудиту. Целями первоначального контакта являются: •установление связи и каналов передачи информации с представителями проверяемой организации (необходимо учитывать, что информация является конфиденциальной, поэтому каналы связи должны быть защищенными, например, с использованием криптографических средств); •подтверждение полномочий для проведения аудита, как со стороны аудиторской организации, так и со стороны проверяемой организации; •предоставление информации, касающейся области аудита ИБ (т.е. какие именно системы и подразделения организации должны быть проверены), методов аудита ИБ и состава группы по аудиту ИБ, в том числе технических экспертов; •получение разрешения

на доступ к соответствующим документам для планирования целей и задач, включая записи (должен быть заключен NDA, с каждым конкретным аудитором могут подписываться индивидуальные Соглашения о неразглашении конфиденциальной информации); •определение применяемых к проверяемой организации законодательных и контрактных требований, требований регуляторов, договорных обязательств, а также других требований, относящихся к обеспечению ИБ в проверяемой организации; •подтверждение соглашения с проверяемой организацией относительно степени раскрытия и обращения с информацией, носящей конфиденциальный характер (тот же NDA); •определение необходимых подготовительных мероприятий по аудиту ИБ, включая даты планов-графиков, выделение ресурсов, подготовка необходимых документов и форм; •определение любых областей заинтересованности или озабоченности проверяемой организации в связи с конкретным намеченным аудитом (например, отсутствие определенных систем защиты информации, серьезные уязвимости, слабая защищенность определенных ресурсов, с целью дальнейшего обоснования в дополнительном финансировании).

II. Описание шкалы оценивания

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Работа выполнена в рамках "продвинутого" уровня. Ответы даны верно, четко сформулированные особенности практических решений

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Работа выполнена в рамках "базового" уровня. Большинство ответов даны верно. В части материала есть незначительные недостатки

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Работа выполнена в рамках "порогового" уровня. Основная часть задания выполнена верно. на вопросы углубленного уровня

Оценка: 2
Описание характеристики выполнения знания: Работа не выполнена или выполнена преимущественно неправильно

III. Правила выставления итоговой оценки по курсу

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

Для курсового проекта/работы:

7 семестр

Форма проведения: Защита КП/КР

I. Процедура защиты КП/КР

Курсовая работа предварительно проверяется преподавателем. После того, как выполненная курсовая работа была допущена к защите, преподаватель задает 2-3 вопроса по существу выполненной работы.

II. Описание шкалы оценивания

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Работа выполнена в рамках "продвинутого" уровня. Ответы даны верно, четко сформулированные особенности практических решений

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Работа выполнена в рамках "базового" уровня. Большинство ответов даны верно. В части материала есть незначительные недостатки

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Работа выполнена в рамках "порогового" уровня. Основная часть задания выполнена верно. на вопросы углубленного уровня

Оценка: 2
Описание характеристики выполнения знания: Работа не выполнена или выполнена преимущественно неправильно

III. Правила выставления итоговой оценки по курсу

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