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

Оценочные материалы
по дисциплине
Аудит безопасности информационных систем

Москва
2021

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

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

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
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)
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)

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. ПК-1 Готов обеспечивать защиту информации в автоматизированных системах в процессе их эксплуатации

ПК-1.3 Выполняет мониторинг защищенности информации в автоматизированных системах

ПК-1.4 Выполняет аудит защищенности информации в автоматизированных системах

и включает:

для текущего контроля успеваемости:

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)

БРС дисциплины

9 семестр

Раздел дисциплины	Веса контрольных мероприятий, %								
	Индекс КМ:	КМ-1	КМ-1	КМ-2	КМ-2	КМ-3	КМ-3	КМ-4	КМ-4
	Срок КМ:	4	4	8	8	12	12	15	15
Вводная лекция									
Понятие и виды аудита информационной безопасности			+						
Менеджмент аудита безопасности информационных систем									
Правовые основы аудита информационной безопасности			+				+		
Способы и цели контроля и проверки процессов и систем		+					+		
Виды аудита информационной безопасности		+					+		

Менеджмент аудита информационной безопасности	+					+		
Программа аудита информационной безопасности	+					+		
Особенности проведения аудита безопасности информационных систем								
Основные этапы аудита информационной безопасности			+	+				
Проведение аудита информационной безопасности			+					
Способы оценки информационной безопасности			+	+	+			
Модели оценки информационной безопасности				+			+	
Аудит управления непрерывностью бизнеса			+				+	
Проведение аудита информационной безопасности в организациях банковской системы России			+	+				
Проведение категорирования и аудита информационной безопасности объектов критической информационной инфраструктуры				+				+
Вес КМ:	10	15	10	15	10	15	10	15

$Общая часть/Для промежуточной аттестации$

БРС курсовой работы/проекта

9 семестр

Раздел дисциплины	Веса контрольных мероприятий, %				
	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
	Срок КМ:	4	8	12	16
Р1. Задание на курсовую работу. Введение курсовой работы		+			
Р2. Первая глава основной части курсовой работы			+	+	
Р3. Вторая глава основной части курсовой работы				+	
Р4. 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
ПК-1	ПК-1.З$_{ПК-1}$ Выполняет мониторинг защищенности информации в автоматизированных системах	Знать: –требования нормативных и правовых документов (законы, стандарты, регламенты) в предметной области дисциплины; –основы менеджмента безопасности информационных систем; Уметь: –разрабатывать и управлять программой аудита безопасности информационных систем; –проводить мероприятия по управлению программой безопасности информационных систем;	Тест № 1 (Тестирование) Контрольная работа № 1 (Контрольная работа) Коллоквиум № 1 (Коллоквиум)
ПК-1	ПК-1.4$_{ПК-1}$ Выполняет аудит защищенности информации в автоматизированных системах	Знать: –основы аудита безопасности информационных систем; –особенности практической организации и проведения аудита	Тест № 2 (Тестирование) Контрольная работа № 2 (Контрольная работа) Коллоквиум № 2 (Коллоквиум) Коллоквиум № 3 (Коллоквиум) Коллоквиум № 4 (Коллоквиум)

		безопасности информационных систем. Уметь: –проводить основные организационные мероприятия по проведению аудита безопасности информационных систем; –осуществлять оценку соответствия информационной безопасности предприятия; –оформлять необходимые документы в рамках аудита безопасности информационных систем.	

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. Контрольная работа № 1

Формы реализации: Письменная работа
Тип контрольного мероприятия: Контрольная работа
Вес контрольного мероприятия в БРС: 10
Процедура проведения контрольного мероприятия: Дается письменное задание, по вариантам. Время работы - до 20 минут.

Краткое содержание задания:
Дать правильные ответы на заданные вопросы.

Контрольные вопросы/задания:

Знать: –основы менеджмента безопасности информационных систем;	1.*В чем состоит проблема доверия к мерам информационной безопасности?*

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: Даны правильные ответы на все поставленные вопросы. Возможна одна небольшая неточность.

Оценка: 4
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Возможен один неправильный ответ, либо две небольшие неточности.

Оценка: 3
Нижний порог выполнения задания в процентах: 40
Описание характеристики выполнения знания: Один полностью правильный ответ, либо неточности в каждом ответе.

КМ-1. Тест № 1

Формы реализации: Письменная работа
Тип контрольного мероприятия: Тестирование
Вес контрольного мероприятия в БРС: 15
Процедура проведения контрольного мероприятия: Тест состоит их 5 вопросов, на каждый может быть от 1 до 4 ответов. На проведение теста дается 15 минут.

Краткое содержание задания:
Дать ответ на заданные вопросы

Контрольные вопросы/задания:

Знать: –требования нормативных и правовых документов (законы, стандарты, регламенты) в предметной области дисциплины;	1.*Оценка эффективности деятельности или качества изделия в обязательном порядке требует:…*

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: Даны правильные ответы на все вопросы, возможна несущественная ошибка

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Возможен неправильный ответ на 1-2 вопроса

Оценка: 3
Нижний порог выполнения задания в процентах: 40
Описание характеристики выполнения знания: Возможен неправильный ответ на 3 вопроса

КМ-2. Контрольная работа № 2

Формы реализации: Компьютерное задание
Тип контрольного мероприятия: Контрольная работа
Вес контрольного мероприятия в БРС: 10
Процедура проведения контрольного мероприятия: Дается письменное задание, по вариантам. Время работы - до 20 минут.

Краткое содержание задания:
Дать правильные ответы на заданные вопросы.

Контрольные вопросы/задания:

Знать: –особенности практической организации и проведения аудита безопасности информационных систем.	1.*Формирование группы аудита безопасности информационных систем, распределение ролей в группе.*

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: Даны правильные ответы на все поставленные вопросы. Возможна одна небольшая неточность.

Оценка: 4
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Возможен один неправильный ответ, либо две небольшие неточности.

Оценка: 3
Нижний порог выполнения задания в процентах: 40
Описание характеристики выполнения знания: Один полностью правильный ответ, либо неточности в каждом ответе.

КМ-2. Тест № 2

Формы реализации: Письменная работа
Тип контрольного мероприятия: Тестирование
Вес контрольного мероприятия в БРС: 15

Процедура проведения контрольного мероприятия: Тест состоит их 5 вопросов, на каждый может быть от 1 до 4 ответов. На проведение теста дается 15 минут.

Краткое содержание задания:
Дать ответ на заданные вопросы

Контрольные вопросы/задания:

Знать: –основы аудита безопасности информационных систем;	1.*Руководство проверяемой организации несет ответственность за:…*

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: Даны правильные ответы на все вопросы, возможна несущественная ошибка

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Возможен неправильный ответ на 1-2 вопроса

Оценка: 3
Нижний порог выполнения задания в процентах: 40
Описание характеристики выполнения знания: Возможен неправильный ответ на 3 вопроса

КМ-3. Коллоквиум № 2

Формы реализации: Письменная работа
Тип контрольного мероприятия: Коллоквиум
Вес контрольного мероприятия в БРС: 10
Процедура проведения контрольного мероприятия: Выполняется практическое задание, по рекомендациям преподавателя

Краткое содержание задания:
Преподаватель выдает практическое задание (кейс) по заданной теме

Контрольные вопросы/задания:

Уметь: –проводить основные организационные мероприятия по проведению аудита безопасности информационных систем;	1.определить требования к защите информации в ходе аудита информационной безопасности и обеспечению конфиденциальности информации аудита.

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: Задание полностью и правильно выполнено, возможны небольшие неточности (1-2)

Оценка: 4
Нижний порог выполнения задания в процентах: 75
Описание характеристики выполнения знания: Задание в основном выполнено, возможны одна существенная ошибка или несколько неточностей.

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Задание выполнено частично, возможны 2-3 ошибки.

КМ-3. Коллоквиум № 1

Формы реализации: Письменная работа
Тип контрольного мероприятия: Коллоквиум
Вес контрольного мероприятия в БРС: 15
Процедура проведения контрольного мероприятия: Выполняется практическое задание, по рекомендациям преподавателя

Краткое содержание задания:
Преподаватель выдает практическое задание (кейс) по заданной теме

Контрольные вопросы/задания:

Уметь: –проводить мероприятия по управлению программой безопасности информационных систем;	1.*определить цель программы аудита и каждого конкретного аудита информационной безопасности;*
Уметь: –разрабатывать и управлять программой аудита безопасности информационных систем;	1.*установить процедуры управления программой аудита информационной безопасности.*

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: Задание полностью и правильно выполнено, возможны небольшие неточности (1-2)

Оценка: 4
Нижний порог выполнения задания в процентах: 75
Описание характеристики выполнения знания: Задание в основном выполнено, возможны одна существенная ошибка или несколько неточностей.

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Задание выполнено частично, возможны 2-3 ошибки.

КМ-4. Коллоквиум № 4

Формы реализации: Письменная работа
Тип контрольного мероприятия: Коллоквиум
Вес контрольного мероприятия в БРС: 10
Процедура проведения контрольного мероприятия: Выполняется практическое задание, по рекомендациям преподавателя

Краткое содержание задания:
Преподаватель выдает практическое задание (кейс) по заданной теме

Контрольные вопросы/задания:

Уметь: –оформлять необходимые документы в рамках аудита безопасности информационных систем.	1.оформить отчет по аудиту информационной безопасности по результатам, полученным в ходе коллоквиума № 3;

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: Задание полностью и правильно выполнено, возможны небольшие неточности (1-2)

Оценка: 4
Нижний порог выполнения задания в процентах: 75
Описание характеристики выполнения знания: Задание в основном выполнено, возможны одна существенная ошибка или несколько неточностей.

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Задание выполнено частично, возможны 2-3 ошибки.

КМ-4. Коллоквиум № 3

Формы реализации: Письменная работа
Тип контрольного мероприятия: Коллоквиум
Вес контрольного мероприятия в БРС: 15
Процедура проведения контрольного мероприятия: Выполняется практическое задание, по рекомендациям преподавателя

Краткое содержание задания:
Преподаватель выдает практическое задание (кейс) по заданной теме

Контрольные вопросы/задания:

Уметь: –осуществлять оценку соответствия информационной безопасности предприятия;	1.провести оценку соответствия информационной безопасности по указанным преподавателем групповым показателям и рассчитать их значения;

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: Задание полностью и правильно выполнено, возможны небольшие неточности (1-2)

Оценка: 4
Нижний порог выполнения задания в процентах: 75
Описание характеристики выполнения знания: Задание в основном выполнено, возможны одна существенная ошибка или несколько неточностей.

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Задание выполнено частично, возможны 2-3 ошибки.

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

9 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

_____2021 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: ПК-1.З$_{ПК-1}$ Выполняет мониторинг защищенности информации в автоматизированных системах

Вопросы, задания

1.Проблема доверия к мерам информационной безопасности. Методологические подходы к решению проблемы оценки информационной безопасности. Достоинства и недостатки подходов.

2.Определение возможности проведения аудита безопасности информационных систем. Факторы, влияющие на возможность проведения аудита.

3. Основные этапы проведения аудита информационной безопасности.

Материалы для проверки остаточных знаний

1.Компетентность лица, ответственного за управление программой аудита информационной безопасности.

Ответы:

Ответ дается в письменной форме, возможны уточняющие вопросы преподавателя.

Верный ответ: Лицо, ответственное за управление программой аудита ИБ, должно быть достаточно компетентным для эффективного и результативного управления программой аудита и связанными с ней рисками, а также иметь следующие знания и навыки: •принципов, процедур, методов и технических средств проведения аудита ИБ; •документов системы менеджмента ИБ и других необходимых для работы документов; •продукции и процессов организации; •применяемых законодательных

и других требований, относящихся к деятельности и/или продукции организации, подлежащей аудиту; •потребителей, поставщиков и других заинтересованных сторон проверяемой организации, где это применимо. Необходимо, чтобы лицо, ответственное за управление программой аудита ИБ, участвовало в мероприятиях по постоянному повышению своего профессионального уровня для того, чтобы поддерживать на должном уровне свои знания и навыки, необходимые для управления программой аудита ИБ.

2.ГОСТ Р ИСО 19011. Руководящие указания по аудиту систем менеджмента. Цели и задачи стандарта, основные положения.

Ответы:

Ответ дается в письменной форме, возможны уточняющие вопросы преподавателя.

Верный ответ: В ИСО 19011 «Руководящие указания по аудиту систем менеджмента» представлено руководство по менеджменту программ аудита, проведению внутренних или внешних аудитов систем менеджмента, а также по вопросу компетентности и оценки аудиторов систем менеджмента. Стандарт не устанавливает требований, а содержит руководящие указания по управлению программой аудита, планированию и проведению аудита системы менеджмента, а также по вопросам компетентности и оценивания аудитора и группы по аудиту. Стандарт предназначен для широкого круга потенциальных пользователей, включающих в себя аудиторов, организации, внедряющие системы менеджмента, и организации, нуждающиеся в проведении аудитов систем менеджмента согласно контрактным или другим обязательствам. Стандарт вводит понятие риска применительно к аудиту систем менеджмента. Применяемый здесь подход относится как к рискам, связанным с недостижением процессом аудита поставленных целей, так и к рискам, связанным с возможностью помешать осуществлению деятельности и процессов проверяемой организации из-за проведения мероприятий по аудиту. При этом не дается отдельного руководства по процессу управления рисками для организации, но признается то, что при проведении аудита организации могут сосредоточить свои усилия на наиболее важных вопросах для системы менеджмента. Настоящим стандартом принимается подход, называемый "комплексным аудитом", при котором две или несколько систем менеджмента, охватывающие различные аспекты менеджмента, проверяются совместно. В случаях, когда эти системы интегрированы в одну систему менеджмента, принципы и процессы проведения аудита будут такими же, как и для комплексного аудита.

2. Компетенция/Индикатор: ПК-1.4$_{ПК-1}$ Выполняет аудит защищенности информации в автоматизированных системах

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

6.Принципы аудита безопасности информационных систем. Дать комментарии по каждому принципу.
7.Виды аудита безопасности информационных систем. Цели и решаемые задачи по каждому виду аудита.
8.Основные способы аудита безопасности информационных систем. Дать комментарии, привести примеры.
9.Комплексный аудит безопасности информационных систем. Цели, решаемые задачи. Особенности проведения.
10.Активный аудит информационной безопасности. Разновидности аудита, решаемые задачи.
11.Процесс оценивания. Схема процесса оценивания. Основные элементы процесса оценивания.
12.Входные и выходные данные оценки безопасности информационных систем. Привести примеры.
13.Модель процесса оценки безопасности информационных систем. Мероприятия процесса оценки.
14.Роли и обязанности ответственных лиц по проведению оценки соответствия.
15.ГОСТ Р ИСО 19011. Руководящие указания по аудиту систем менеджмента. Цели и задачи стандарта, основные положения.
16.Программа аудита информационной безопасности. Содержание программы. Управление программой аудита.
17.Цели и объем программы аудита информационной безопасности. Риски программы информационной безопасности.
18.Планирование программы аудита информационной безопасности. Особенности планирования. Ресурсы программы аудита.
19.Внедрение программы аудита информационной безопасности: перечислить задачи, дать комментарии по каждой задаче.
20.Контроль и совершенствование программы аудита информационной безопасности.
21.Компетентность лица, ответственного за управление программой аудита информационной безопасности.
22.Типовые действия при проведении аудита. Дать комментарии по каждому этапу проведения аудита.
23.Первоначальный контакт аудиторской организации с проверяемой организацией. Цели и задачи первоначального контакта.
24.Порядок формирования группы по аудиту информационной безопасности. Компетентность и оценка аудиторов.
25.Процессная модель аудита информационной безопасности. Перечислить этапы и содержание каждого этапа.
26. Менеджмент аудита информационной безопасности. Понятие, модель, ответственные лица, особенности.
27.Осознание аудита информационной безопасности. Цели, входные и выходные данные. Основные мероприятия.
28.Организация проведения аудита информационной безопасности.
29.План проведения аудита информационной безопасности. Содержание плана. Особенности его подготовки и внедрения
30.Проведение аудита информационной безопасности на месте. Сбор и анализ исходных данных при проведении аудита.
31.Методы сбора информации при проведении аудита информационной безопасности. Свидетельства аудита. Верификация данных.
32.Выводы аудита информационной безопасности. Формирование заключения по аудиту. Рекомендации по результатам аудита.
33.Отчет по аудиту. Содержание отчета. Подготовка и рассылка отчета по аудиту.

34.Завершение аудита информационной безопасности. Вопросы, решаемые в ходе заключительного совещания.
35.Оценивание информационной безопасности на основе показателей информационной безопасности.
36.Оценивание информационной безопасности на основе моделей зрелости процессов обеспечения информационной безопасности
37.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).

2.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.

3.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.

II. Описание шкалы оценивания

Оценка: 5

Нижний порог выполнения задания в процентах: 90

Описание характеристики выполнения знания: Даны полные и правильные ответы на поставленные вопросы. Возможна одна небольшая неточность.

Оценка: 4

Нижний порог выполнения задания в процентах: 70

Описание характеристики выполнения знания: Даны в целом правильные ответы, возможна одна ошибка, либо две-три небольшие неточности.

Оценка: 3

Нижний порог выполнения задания в процентах: 40

Описание характеристики выполнения знания: Дан правильный ответ на один вопрос, либо имеются ошибки в обеих ответах на вопросы.

III. Правила выставления итоговой оценки по курсу

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

Для курсового проекта/работы:

9 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: 90
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: 70
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

III. Правила выставления итоговой оценки по курсу

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