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
2022

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. 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. 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. КМ-1 (Тестирование)

БРС дисциплины

9 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.		+		
3. 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

9 семестр

Раздел дисциплины	Веса контрольных мероприятий, %				
	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
	Срок КМ:	4	8	12	16
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 № 2. 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)
ПК-10	ПК-10(Компетенция)	Уметь: участвовать в работах по реализации политики информационной безопасности; проводить анализ информационной	Практическое задание № 2. 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

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

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. Система менеджмента аудита безопасности информационных систем. КМ-1

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.*Что относится к принципам 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

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. *Программа 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

КМ-3. Практическое задание № 2. 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:

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.*Документация системы менеджмента аудита безопасности информационных систем.*
Уметь: участвовать в работах по реализации политики информационной безопасности;	1.*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

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: проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов, разрабатывать предложения по совершенствованию системы управления информационной безопасностью;	1.определить порядок рассылки и хранения отчета по аудиту 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

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

_____2018 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.Необходимость в проведении аудита безопасности информационных систем. Дать комментарии, привести примеры.
2.Виды аудита безопасности информационных систем. Цели и решаемые задачи по каждому виду аудита.
3.Модель процесса оценки безопасности информационных систем. Мероприятия процесса оценки.
4.ГОСТ Р ИСО 19011. Руководящие указания по аудиту систем менеджмента. Цели и задачи стандарта, основные положения.
5.Компетентность лица, ответственного за управление программой аудита информационной безопасности.

Материалы для проверки остаточных знаний

1.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.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.Роли и обязанности ответственных лиц по проведению оценки соответствия.

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

3.Цели и объем программы аудита информационной безопасности. Риски программы информационной безопасности.

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

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.

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

Вопросы, задания

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

2.Понятие аудита. Понятия «Аудит безопасности информационных систем» и «Аудит информационной безопасности». Область каждого из аудитов, цели, решаемые задачи.

3.Основные стандарты в области аудита безопасности информационных систем. Содержание (кратко) и область действия стандартов.

4.Требования законодательства Российской Федерации и нормативных документов регулирующих органов по проведению аудита (оценки соответствия) в области информационной безопасности.

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.Основные способы аудита безопасности информационных систем. Дать комментарии, привести примеры.

8.Комплексный аудит безопасности информационных систем. Цели, решаемые задачи. Особенности проведения.

9.Активный аудит информационной безопасности. Разновидности аудита, решаемые задачи.

10.Процесс оценивания. Схема процесса оценивания. Основные элементы процесса оценивания.

11.Входные и выходные данные оценки безопасности информационных систем. Привести примеры.

12.Планирование программы аудита информационной безопасности. Особенности планирования. Ресурсы программы аудита.

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

14.Контроль и совершенствование программы аудита информационной безопасности.

15.Типовые действия при проведении аудита. Дать комментарии по каждому этапу проведения аудита.
16.Первоначальный контакт аудиторской организации с проверяемой организацией. Цели и задачи первоначального контакта.
17.Порядок формирования группы по аудиту информационной безопасности. Компетентность и оценка аудиторов.
18.Процессная модель аудита информационной безопасности. Перечислить этапы и содержание каждого этапа.
19. Менеджмент аудита информационной безопасности. Понятие, модель, ответственные лица, особенности.
20.Осознание аудита информационной безопасности. Цели, входные и выходные данные. Основные мероприятия.
21. Основные этапы проведения аудита информационной безопасности.
22.Организация проведения аудита информационной безопасности.
23.План проведения аудита информационной безопасности. Содержание плана. Особенности его подготовки и внедрения
24.Проведение аудита информационной безопасности на месте. Сбор и анализ исходных данных при проведении аудита.
25.Методы сбора информации при проведении аудита информационной безопасности. Свидетельства аудита. Верификация данных.
26.Выводы аудита информационной безопасности. Формирование заключения по аудиту. Рекомендации по результатам аудита.
27.Отчет по аудиту. Содержание отчета. Подготовка и рассылка отчета по аудиту.
28.Завершение аудита информационной безопасности. Вопросы, решаемые в ходе заключительного совещания.
29.Оценивание информационной безопасности на основе показателей информационной безопасности.
30.Оценивание информационной безопасности на основе моделей зрелости процессов обеспечения информационной безопасности
31.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

III. Правила выставления итоговой оценки по курсу

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

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: 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

III. Правила выставления итоговой оценки по курсу

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