Министерство науки и высшего образования РФ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Национальный исследовательский университет «МЭИ»

Направление подготовки/специальность: 38.03.02 Менеджмент

Наименование образовательной программы: Менеджмент предприятий и организаций

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очная

Оценочные материалы
по дисциплине
Теория информационной безопасности

Москва
2022

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Преподаватель	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Унижаев Н.В. Идентификатор: Rb43f42d6-UnizhayevNV-2454ef2(	Н.В. Унижаев
(должность)	(подпись)	(расшифровка подписи)

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Коробко М.О. Идентификатор: R22a1a9d4-KorobkoMO-fab3716e	М.О. Коробко
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)
Заведующий выпускающей кафедры	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Кетоева Н.Л. Идентификатор: R56dba1ba-KetoyevaNL-5403d8c5	Н.Л. Кетоева
(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. УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач

ИД-1 Выполняет поиск необходимой информации, её критический анализ и обобщает результаты анализа для решения поставленной задачи

и включает:

для текущего контроля успеваемости:

Форма реализации: Выполнение задания

1. Практическое задание № 1 Оценка ценности информации на основе анализа рисков информационной безопасности. Индивидуальное практическое задание № 1 Анализ общедоступной базы уязвимостей (Отчет)
2. Практическое задание № 2. Неформальные модели безопасности. Модель MMS. Общая информация, ограничения модели. Частные случаи действия моделей. Индивидуальное практическое задание № 2. Разработка «Модели угроз безопасности информации организации «Х» (Отчет)

Форма реализации: Выступление (доклад)

1. Практическое задание № 5. Анализ РД ФСТЭК «Концепция защиты средств вычислительной техники и автоматизированных систем от НСД к информации» (Доклад)

Форма реализации: Защита задания

1. Практическое задание № 3. Основная теорема безопасности Белла – Лападулы. Постановка задачи, формулировка и доказательство. 4.Практическое задание № 4. Сравнительный анализ БЛМ – БМ. Общее и основные различия в моделях. Возможность создания на их основе моделей контроля конфиденциальности и целостности (Отчет)

БРС дисциплины

3 семестр

Раздел дисциплины	Веса контрольных мероприятий, %				
	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
	Срок КМ:	4	8	12	15
Основы теории обеспечения информационной безопасности					
Вводная тема.		+			

Тема 1. Информация, как наиболее ценный ресурс современного общества.	+			
Тема 2. Понятие угрозы безопасности информации.	+	+		
Тема 3. Понятие уязвимости в информационной безопасности.	+	+		
Тема 4. Понятие нарушителя и классификационные признаки нарушителей ИБ.	+	+		
Тема 5. Модель угроз: понятие, цель разработки, выполняемые задачи.		+	+	
Методологические основы защиты информации				
Тема 6. Понятие, общие положения, модели безопасности		+	+	
Тема 7. Модель ХРУ (HRU).			+	
Тема 8. Мандатная Модель целостности Биба (БМ).			+	
Тема 9. Оценка взглядов субъектов информационных отношений на обеспечение конфиденциальности информации.				+
Тема 10. Анализ причин и методов НСД к информации.				+
Тема 11. Характеристика методов и средств защиты информации.				+
Тема 12. Методологические подходы к защите информации и принципы её организации.				+
Вес КМ:	25	25	25	25

$Общая часть/Для промежуточной аттестации$

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
УК-1	ИД-1$_{УК-1}$ Выполняет поиск необходимой информации, её критический анализ и обобщает результаты анализа для решения поставленной задачи	Знать: критерии мотивации к выполнению профессиональной деятельности состав и перечень защищаемой информации, классификацию ее по видам тайны информации, носителям информации, а также угрозы и уязвимости и возможные пути их реализации источники, способы и результаты дестабилизирующего воздействия на защищаемую информацию нормативные методические документы федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в	Практическое задание № 1 Оценка ценности информации на основе анализа рисков информационной безопасности. Индивидуальное практическое задание № 1 Анализ общедоступной базы уязвимостей (Отчет) Практическое задание № 2. Неформальные модели безопасности. Модель MMS. Общая информация, ограничения модели. Частные случаи действия моделей. Индивидуальное практическое задание № 2. Разработка «Модели угроз безопасности информации организации «Х» (Отчет) Практическое задание № 3. Основная теорема безопасности Белла – Лападулы. Постановка задачи, формулировка и доказательство. 4.Практическое задание № 4. Сравнительный анализ БЛМ – БМ. Общее и основные различия в моделях. Возможность создания на их основе моделей контроля конфиденциальности и целостности (Отчет) Практическое задание № 5. Анализ РД ФСТЭК «Концепция защиты средств вычислительной техники и автоматизированных систем от НСД к информации» (Доклад)

		данной области Уметь: выполнять профессиональную деятельность в области обеспечения информационной безопасности применять теоретические знания в области информационной безопасности на основе системного анализа и системного подхода способностью формирования различных моделей контроля конфиденциальности и целостности	

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. Практическое задание № 1 Оценка ценности информации на основе анализа рисков информационной безопасности. Индивидуальное практическое задание № 1 Анализ общедоступной базы уязвимостей

Формы реализации: Выполнение задания
Тип контрольного мероприятия: Отчет
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Самостоятельное выполнение практического занятия.

Краткое содержание задания:
Используя информацию общедоступных интернет - ресурсов провести анализ понятия «тайна информации» и найти в законодательстве Российской Федерации явные упоминания о видах тайны информации (конфиденциальной информации).

Контрольные вопросы/задания:

Знать: критерии мотивации к выполнению профессиональной деятельности	1.1. Понятие ценности информации, свойства информации, определяющие ее ценность.
Знать: состав и перечень защищаемой информации, классификацию ее по видам тайны информации, носителям информации, а также угрозы и уязвимости и возможные пути их реализации	1.2. Методы определения ценности информации (личной, корпоративной и государственной).

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 № 2. Неформальные модели безопасности. Модель MMS. Общая информация, ограничения модели. Частные случаи действия моделей. Индивидуальное практическое задание № 2. Разработка «Модели угроз безопасности информации организации «Х»

Формы реализации: Выполнение задания
Тип контрольного мероприятия: Отчет
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Самостоятельное выполнение практического занятия.

Краткое содержание задания:
Используя материалы лекции по теме 4 (учебный вопрос 2) и интернет - ресурсы разработать информационную систему поддержки практической работы с профилактикой нарушений режима ИБ в организации ПАО «Сигма».

Контрольные вопросы/задания:

Знать: источники, способы и результаты дестабилизирующего воздействия на защищаемую информацию	1.1.Модель угроз: понятие, цель разработки, выполняемые задачи. 2.2.Требования к разработке Модели угроз.
Уметь: применять теоретические знания в области информационной безопасности на основе системного анализа и системного подхода	1.1. Последовательность работ по моделированию угроз. 2.2. Содержание Модели угроз 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 № 3. Основная теорема безопасности Белла – Лападулы. Постановка задачи, формулировка и доказательство. 4.Практическое задание № 4. Сравнительный анализ БЛМ – БМ. Общее и основные различия в моделях. Возможность создания на их основе моделей контроля конфиденциальности и целостности

Формы реализации: Защита задания
Тип контрольного мероприятия: Отчет
Вес контрольного мероприятия в БРС: 25

Процедура проведения контрольного мероприятия: Самостоятельное выполнение практического занятия.

Краткое содержание задания:

Используя материалы лекции по теме 7 разработать модель управления конфиденциальностью информации для информационной системы малого предприятия «Х» на основе положений моделей ХРУ - БЛМ.

Контрольные вопросы/задания:

Уметь: способностью формирования различных моделей контроля конфиденциальности и целостности	1.1. Модель ХРУ (HRU). Исходные данные модели. 2.2. Модель БЛ (BL). Исходные данные.

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 № 5. Анализ РД ФСТЭК «Концепция защиты средств вычислительной техники и автоматизированных систем от НСД к информации»

Формы реализации: Выступление (доклад)
Тип контрольного мероприятия: Доклад
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Самостоятельное выполнение практического занятия.

Краткое содержание задания:

Краткая характеристика государственной системы защиты информации Российской Федерации. Анализ ее структуры, задач и полномочий.

Контрольные вопросы/задания:

Знать: нормативные методические документы федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной	1.1.Оценка взглядов субъектов информационных отношений на обеспечение конфиденциальности информации. 2.2. Оценка взглядов субъектов информационных отношений на обеспечение доступности и целостности информации. 3.3. Оценка взглядов субъектов информационных

области	отношений на обеспечение безопасности информации.
Уметь: выполнять профессиональную деятельность в области обеспечения информационной безопасности	1.Сравнительный анализ методов организации работ по защите информационных активов.

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

3 семестр

Форма промежуточной аттестации: Зачет

Пример билета

1. Раскрыть понятие «тайна». Характеристика видов тайны информации. Привести примеры.
2. Характеристика порядка определения актуальных угроз безопасности информации согласно требований руководящих документов ФСТЭК.
3. Характеристика элементарных операций перехода системы из одного состояния в другое в дискреционной модели Харисона-Рузо-Ульмана.

Процедура проведения

Письменный ответ

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

1. Компетенция/Индикатор: ИД-1$_{УК-1}$ Выполняет поиск необходимой информации, её критический анализ и обобщает результаты анализа для решения поставленной задачи

Вопросы, задания

1.1. Понятие ценности информации, свойства информации, определяющие ее ценность.
2.2. Методы определения ценности информации (личной, корпоративной и государственной).
3.3. Понятие тайны информации и современное состояние тайны информации в РФ.
4.4. Виды доступа к информации. Организация доступа к общедоступной информации в РФ.
5.5. Информация ограниченного доступа. Несанкционированный доступ к информации.
6.6. Понятие угрозы безопасности информации.
7.7. Понятие угрозы безопасности информации. Основы классификации угроз.
8.8. Классификация угроз по характеру воздействия, расположению источника угроз, составляющим ИБ, составляющим ИБ.
9.9. Моделирование и разработка модели угроз
10.10. Понятие уязвимости и природа (причины) возникновения уязвимостей в ИС.
11.11. Классификация уязвимостей по типу, компоненту содержащему уязвимость, этапам жизненного цикла, преднамеренности внесения, месту в ИС.
12.12. Основные понятие, назначение и работа с базами уязвимостей.
13.13. Понятие нарушителя и классификационные признаки нарушителей ИБ.
14.14. Общая характеристика внутренних и внешних нарушителей.
15.15. Классификация нарушителей по используемым средствам и методам, уровню подготовки (квалификации).
16.16. Характеристика основных групп нарушителей
17.17. Общая характеристика модели нарушителя: понятие, назначение. цели.
18.18. Структура модели нарушителя: основные разделы и содержание
19.19. Системный подход к моделированию угроз безопасности информации.

20.20. Модель угроз: понятие, цель разработки, выполняемые задачи.
21.21. Последовательность работ по моделированию угроз
22.22. Содержание «Модели угроз безопасности информации организации»
23.23. Оценка вероятности (возможности) реализации угроз безопасности информации
24.24. Оценка степени возможного ущерба от реализации угрозы безопасности информации
25.25. Определение актуальности угрозы безопасности информации
26.26. Понятие, общие положения, модели безопасности.
27.27. Модели Политик безопасности.
28.28. Классификация и содержание основных моделей безопасности.
29.29. Понятие и сущность Политики безопасности. Дуализм политики.
30.30. Формальное и неформальное выражение Политики безопасности. Виды и характеристика Политик безопасности. Дискреционная, мандатная политика, политика безопасности информационных потоков, ролевого доступа и изолированной среды.
31.31. Постановка и описание дискреционной модели Харрисона-Руззо-Ульмана.
32.32. Постановка и описание мандатной модели Белла-Лападулы.
33.33. Постановка и описание модели Биба.
34.34. Постановка и описание модели целостности Кларка – Вильсона.
35.35. Постановка и описание модели целостности MMS (военных сообщений).
36.36. Постановка и описание модели Take-Grant.
37.37. Проблемы развития теории и практики обеспечения информационной безопасности
38.38. Интерпретация понятия информационной безопасности

Материалы для проверки остаточных знаний

1.**1. Какие свойства информации определены моделью CIA?**

Ответы:

1. Источники информации
2. Потребители информации
3. Собственники информации
4. Регулирующие органы
5. Владельцы систем обработки информации
6. Все вышеперечисленные

Верный ответ: 6

2.**2. Кто из перечисленных категорий не является субъектом информационных отношений?**

Ответы:

1. Источники информации
2. Потребители информации
3. Собственники информации
4. Регулирующие органы
5. Владельцы систем обработки информации
6. Все вышеперечисленные

Верный ответ: 4

3.**3. Модель Белла-Лападулы относится к…**

Ответы:

1. Дискреционным моделям
2. Мандатным моделям
3. Ролевым моделям
4. Неформальным моделям
5. Моделям контроля целостности

Верный ответ: 2

4.**4. Какой классификационный признак уязвимости лишний?**

Ответы:

1. Уязвимости в аппаратуре ИС
2. Уязвимости, связанные с пользователем ИС
3. Уязвимости в системном ПО
4. Уязвимости в прикладном ПО

Верный ответ: 2

5.**5. Какие пункты не входят в Модель угроз безопасности информации организации?**

Ответы:

1. Описание ИС
2. Описание угроз
3. Описание возможностей нарушителя
4. Описание способов реализации угроз
5. Описание последствий нарушений
6. Описание порядка ликвидации последствий
7. Все перечисленные входят

Верный ответ: 6

6.**6. Сформулируйте цель разработки Модели угроз безопасности…**

Ответы:

-

Верный ответ: Целью разработки модели угроз является организационное и методическое обеспечение мероприятий способствующих научно обоснованному построению системы их нейтрализации (построению СОИБ) в ИС (АС) организации.

7.**7. Какие пункты не входят в Модель угроз безопасности информации организации?**

Ответы:

1. Описание ИС
2. Описание угроз
3. Описание возможностей нарушителя
4. Описание способов реализации угроз
5. Описание последствий нарушений
6. Описание порядка ликвидации последствий
7. Все перечисленные входят

Верный ответ: 6

8.**8. Интерпретация правил модели BLM**

Ответы:

1. Нет записи вверх и нет записи вниз
2. Нет записи вверх и нет чтения вниз
3. Нет чтения вниз и нет чтения вверх
4. Нет записи вниз и нет чтения вверх

Верный ответ: 4

9.**9. Какова правильная кодировка уязвимостей в базе угроз ФСТЭК?**

Ответы:

1. БДУ:2016-01427
2. БДУ: 2016- 01427
3. BDU:2016-01427
4. BDU: 2016- 01427

Верный ответ: 3

10.**10. Какой вид профессиональной тайны информации отсутствует в законодательстве РФ?**

Ответы:

1. Врачебная
2. Адвокатская
3. Военная
4. Следствия
5. Банковская
6. Исповеди

Верный ответ: 3

11.**11. Что не является видом политики безопасности?**

Ответы:

1. Мандатная
2. Дискретная
3. Безопасности информационных потоков
4. Изолированной программной среды
5. Ролевого разграничения доступа

Верный ответ: 2

12.**12. Дайте определение метода защиты информации**

Ответы:

-

Верный ответ: Под методом защиты информации понимается конкретный способ достижения цели, заключающейся в реализации определенной упорядоченной деятельности, направленной на выполнение одного или нескольких механизмов (действий, работ), обеспечивающих состояние безопасности информации

13.**13. Какой признак классификации угроз ИБ лишний?**

Ответы:

1. По характеру воздействия
2. По опасности последствий
3. По составляющим ИБ
4. По компонентам ИС
5. По расположению источника угроз

Верный ответ: 2

14.**14. Сколько правил содержит KVM?**

Ответы:

1. 7
2. 8
3. 9
4. 10

Верный ответ: 3

15.**15. Что не является исходными данными модели ХРУ (HRU)?**

Ответы:

1. Конечное множество субъектов
2. Конечное множество объектов
3. Конечное множество прав доступа
4. Конечное множество элементов матрицы доступа
5. Конечное множество команд
6. Все перечисленные являются

Верный ответ: 4

16.**16. Чем не определяется перечень угроз ИБ?**

Ответы:

1. Перечнем информационных активов;
2. Характером и свойствами информации;
3. Свойствами ИС;
4. Размером ущерба от реализации;

5. Количеством и «качеством» персонала;

Верный ответ: 4

17.**17. Уязвимость информационной системы это**

Ответы:

1. Слабость информационной системы, удовлетворяющая требованиям специальных нормативных документов ФСБ
2. Слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации
3. Совокупность условий и факторов, определяющих потенциально опасные последствия реализации угроз
4. Слабость информационной системы, удовлетворяющая требованиям специальных нормативных документов ФСТЭК

Верный ответ: 2

18.**18. Какова правильная кодировка угроз безопасности в базе угроз ФСТЭК?**

Ответы:

1. УБИ. 001
2. УИБ. 001
3. УБИ.001
4. УИБ.001
5. УБИ.01
6. УИБ.01

Верный ответ: 1

19.**19. Дайте определение НСД к информации**

Ответы:

-

Верный ответ: Несанкционированный доступ (НСД) заключается в получении субъектом (пользователем, нарушителем) доступа к объекту в нарушение правил разграничения доступа, установленных в соответствии с принятой в организации политикой безопасности

20.**20. Каких видов моделей угроз безопасности информации не разрабатывается?**

Ответы:

1. Сертифицированная
2. Базовая
3. Отраслевая
4. Частная
5. Типовая

Верный ответ: 1

21.**21. Какие компоненты ИС рассматриваются при классификации угроз ИБ?**

Ответы:

1. Человек
2. Инфраструктура (территория, здание, помещения);
3. Программное обеспечение
4. Аппаратура
5. 1, 3, 4
6. 1-4

Верный ответ: 5

22.**22. Что не является формальным выражением политики безопасности?**

Ответы:

1. Математическое
2. Текстовое
3. Алгоритмическое
4. Схемотехническое

5. Все перечисленные являются

Верный ответ: 2

23.**23. Модель ХРУ (HRU) относится к…**

Ответы:

1. Дискреционным моделям
2. Мандатным моделям
3. Ролевым моделям
4. Неформальным моделям
5. Моделям контроля целостности

Верный ответ: 1

24.**24. Дайте определение Модели угроз безопасности информации**

Ответы:

-

Верный ответ: Модель угроз безопасности - физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации

25.**25. В чем заключается сущность метки секретности, присвоенной субъекту в BLM?**

Ответы:

1. Определяет его уровень секретности
2. Определяет его уровень надежности
3. Определяет уровень доверия к субъекту
4. Определяет уровень доступа
5. 2 и 4
6. 3 и 4

Верный ответ: 6

26.**26. Что не является классификационным признаком уязвимости ИС?**

Ответы:

1. Тип угрозы, эксплуатирующей уязвимость
2. Преднамеренность внесения уязвимости
3. Тип компонента ИС, содержащего уязвимость
4. Тип уязвимости
5. Место уязвимости в ИС

Верный ответ: 1

27.**27. Модель Биба (BM) относится к…**

Ответы:

1. Дискреционным моделям
2. Мандатным моделям
3. Ролевым моделям
4. Неформальным моделям
5. Моделям контроля конфиденциальности

Верный ответ: 4

28.**28. Какой из перечисленных не относится к методам защиты информации?**

Ответы:

1. Административный
2. Страхование
3. Морально-нравственный
4. Шифрование
5. Дезинформация

Верный ответ: 1

29.**29. Чем характеризуется состояние системы в соответствии с BLM?**

Ответы:

1. Состояние матрицы прав доступа, A
2. Конечное множество прав доступа, F
3. Функция уровня безопасности, R
4. 1 и 2
5. 2 и 3

Верный ответ: 4

30.**30. Какая из перечисленных является неформальной моделью контроля конфиденциальности информации?**

Ответы:

1. MMS
2. TAM
3. RBAC
4. BM

Верный ответ: 1

31.**31. Какой элемент порядковой шкалы ценности информации, составляющей ГТ, лишний;**

Ответы:

1. Секретно
2. Строго секретно
3. Совершенно секретно
4. Особой важности

Верный ответ: 2

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