

**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  
Теория информационной безопасности**

**Москва  
2023**

## ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Разработчик

|  |                                                    |                              |
|--|----------------------------------------------------|------------------------------|
|  | Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» |                              |
|  | Сведения о владельце ЦЭП МЭИ                       |                              |
|  | Владелец                                           | Баронов О.Р.                 |
|  | Идентификатор                                      | R90d76356-BaronovOR-7bf8fd7e |

О.Р. Баронов

## 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-4 способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты
3. ПК-15 способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю
4. ОК-5 способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики

и включает:

**для текущего контроля успеваемости:**

Форма реализации: Выступление (доклад)

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

Форма реализации: Защита задания

1. 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)
2. 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

4 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                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ОПК-7              | ОПК-7(Компетенция) | Знать:<br>состав и перечень защищаемой информации, классификацию ее по видам тайны информации, носителям информации, а также угрозы и уязвимости и возможные пути их реализации<br>Уметь:<br>выполнять профессиональную деятельность в области обеспечения информационной безопасности | Практическое задание № 1 Оценка ценности информации на основе анализа рисков информационной безопасности. Индивидуальное практическое задание № 1 Анализ общедоступной базы уязвимостей (Отчет)<br>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) |
| ПК-4               | ПК-4(Компетенция)  | Знать:<br>источники, способы и результаты дестабилизирующего воздействия на защищаемую информацию<br>Уметь:<br>применять теоретические знания в области                                                                                                                                | Практическое задание № 1 Оценка ценности информации на основе анализа рисков информационной безопасности. Индивидуальное практическое задание № 1 Анализ общедоступной базы уязвимостей (Отчет)<br>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) |

|       |                    |                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                            |
|-------|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       |                    | информационной безопасности на основе системного анализа и системного подхода                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                            |
| ПК-15 | ПК-15(Компетенция) | Знать:<br>нормативные методические документы федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области<br>Уметь:<br>организовывать технологический процесс защиты информации ограниченного доступа | Практическое задание № 5. Анализ РД ФСТЭК «Концепция защиты средств вычислительной техники и автоматизированных систем от НСД к информации» (Доклад)                                                                                                                                                                       |
| ОК-5  | ОК-5(Компетенция)  | Знать:<br>критерии мотивации к выполнению профессиональной деятельности<br>Уметь:<br>способностью формирования различных моделей контроля конфиденциальности и целостности                                                                                                | Практическое задание № 3. Основная теорема безопасности Белла – Лападулы. Постановка задачи, формулировка и доказательство.<br>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) |

## **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:** Выступление (доклад)

**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: источники, способы и результаты дестабилизирующего воздействия на защищаемую информацию   | 1.1. Понятие ценности информации, свойства информации, определяющие ее ценность.<br>2. Методы определения ценности информации (личной, корпоративной и государственной). |
| Уметь: выполнять профессиональную деятельность в области обеспечения информационной безопасности | 1.Порядок оценки ценности информации на основе анализа рисков 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-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:** 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 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: состав и перечень защищаемой информации, классификацию ее по видам тайны информации, носителям информации, а также угрозы и уязвимости и возможные пути их реализации | 1.1. Модель угроз: понятие, цель разработки, выполняемые задачи.<br>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.<br>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*

*Оценка: 2*

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

|                                                                                              |                                                                                                                                                                                                 |
|----------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Знать: критерии мотивации к выполнению профессиональной деятельности                         | 1.1. Модель ХРУ (HRU). Постановка задачи моделирования.<br>2. Модель ХРУ (HRU). Исходные данные модели.<br>3. Модель ХРУ (HRU). Управление доступом. Обеспечение безопасного состояния системы. |
| Уметь: способностью формирования различных моделей контроля конфиденциальности и целостности | 1.1. Модель БЛ (BL). Подходы к моделированию.<br>2. Модель БЛ (BL). Исходные данные.<br>3. Модель БЛ (BL). Характеристика безопасного состояния системы.                                        |

**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 № 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 области | 1.1. Оценка взглядов субъектов информационных отношений на обеспечение конфиденциальности информации.<br>2. Оценка взглядов субъектов информационных отношений на обеспечение доступности и целостности информации.<br>3. Оценка взглядов субъектов информационных отношений на обеспечение безопасности информации. |
| Уметь: организовывать технологический процесс защиты информации ограниченного доступа                                                                                      | 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

*Оценка: 2*

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

# СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

4 семестр

Форма промежуточной аттестации: Экзамен

Пример билета

|                                                                                                                                                                                                                                                                                                       |                                                                                                                                                     |                                                                                                     |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| <b>НИУ МЭИ</b>                                                                                                                                                                                                                                                                                        | <b>ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1</b><br>Кафедра:<br><i>Безопасности и информационных технологий</i><br>Дисциплина: «Теория информационной безопасности» | <i>Утверждаю:<br/>Зав. каф. БИТ<br/>А.Ю.Невский<br/>Протокол кафедры №3<br/>«16» декабря 2020г.</i> |
| 1. Раскрыть понятие «ценность информации». Характеристика свойств ценности информации. Привести примеры.<br>2. Модель угроз безопасности информации понятие, назначение, цели и задачи её разработки в организации.<br>3. Назначение и условия постановки дискреционной модели Харисона-Рузо-Ульмана. |                                                                                                                                                     |                                                                                                     |

## Процедура проведения

Экзамен проводится в письменной форме по билетам согласно программе экзамена

### ***1. Перечень компетенций/индикаторов и контрольных вопросов проверки результатов освоения дисциплины***

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

#### **Вопросы, задания**

- 1.2. Методы определения ценности информации (личной, корпоративной и государственной).
- 2.8. Классификация угроз по характеру воздействия, расположению источника угроз, составляющим ИБ, составляющим ИБ.
- 3.10. Понятие уязвимости и природа (причины) возникновения уязвимостей в ИС.
- 4.15. Классификация нарушителей по используемым средствам и методам, уровню подготовки (квалификации).
- 5.16. Характеристика основных групп нарушителей.

#### **Материалы для проверки остаточных знаний**

##### **1.8. 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

##### **2.12. 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

**3.15. 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

**2. Компетенция/Индикатор: ПК-4(Компетенция)**

**Вопросы, задания**

- 1.9. Моделирование и разработка модели угроз.
- 2.19. Системный подход к моделированию угроз безопасности информации.
- 3.22. Содержание «Модели угроз безопасности информации организации».
- 4.27. Модели Политик безопасности.
- 5.30. Формальное и неформальное выражение Политики безопасности. Виды и характеристика Политик безопасности. Дискреционная, мандатная политика, политика безопасности информационных потоков, ролевого доступа и изолированной среды.
- 6.31. Постановка и описание дискреционной модели Харрисона-Руззо-Ульмана.
- 7.34. Постановка и описание модели целостности Кларка – Вильсона.
- 8.35. Постановка и описание модели целостности MMS (военных сообщений).

**Материалы для проверки остаточных знаний**

**1.7. 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

**2.10. 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

**3.17. 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

### **3. Компетенция/Индикатор: ПК-15(Компетенция)**

#### **Вопросы, задания**

- 1.20. Модель угроз: понятие, цель разработки, выполняемые задачи.
- 2.21. Последовательность работ по моделированию угроз.
- 3.23. Оценка вероятности (возможности) реализации угроз безопасности информации.
- 4.25. Определение актуальности угрозы безопасности информации.
- 5.32. Постановка и описание мандатной модели Белла-Лападулы.

#### **Материалы для проверки остаточных знаний**

**1.9. 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

**2.24. 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

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

Ответы:

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

Верный ответ: 1

### **4. Компетенция/Индикатор: ОК-5(Компетенция)**

#### **Вопросы, задания**

- 1.1. Понятие ценности информации, свойства информации, определяющие ее ценность.
- 2.3. Понятие тайны информации и современное состояние тайны информации в РФ.
- 3.4. Виды доступа к информации. Организация доступа к общедоступной информации в РФ.
- 4.6. Понятие угрозы безопасности информации.
- 5.7. Понятие угрозы безопасности информации. Основы классификации угроз.
- 6.13. Понятие нарушителя и классификационные признаки нарушителей ИБ.

#### **Материалы для проверки остаточных знаний**

**1.2. 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

**2.11. Дайте определение метода защиты информации**

Ответы:

-

Верный ответ: -

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

Ответы:

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

Верный ответ: 1

**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 определяется в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ» на основании семестровой и экзаменационной составляющих.