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 компьютерных систем

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очная

Оценочные материалы
по дисциплине
Основы информационной безопасности

Москва
2021

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Преподаватель	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Потехецкий С.В. Идентификатор: R83b30a44-PotekhetskySV-31b213(	С.В. Потехецкий
(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-1 способностью анализировать физические явления и процессы для решения профессиональных задач

2. 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

и включает:

для текущего контроля успеваемости:

Форма реализации: Билеты (письменный опрос)

1. Тест № 3; Тест № 4 (Тестирование)
2. Тест №5 (Тестирование)
3. Тест №6 (Тестирование)

Форма реализации: Проверка задания

1. Тест № 1; Тест № 2 (Тестирование)

БРС дисциплины

1 семестр

Раздел дисциплины	Веса контрольных мероприятий, %				
	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
	Срок КМ:	4	8	12	15
Основные составляющие информационной безопасности					
Вводная лекция		+	+	+	+
Тема 2. Основы системы информационной безопасности		+		+	+
Базовые основы защиты информации					
Тема 3. Организационно-правовое и кадровое обеспечение системы информационной безопасности			+		+
Тема 4.Финансово-экономическое обеспечение системы информационной безопасности			+		+

Тема 5. Инженерно-техническое обеспечение системы информационной безопасности	+	+	+	
Тема 6. Программно-аппаратное обеспечение системы информационной безопасности	+	+	+	
Тема 7. Аудит системы информационной безопасности		+		+
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-1	ОПК-1(Компетенция)	Знать: анализировать физические явления и процессы, применяемые для обеспечения информационной безопасности объекта защиты 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	Тест № 3; Тест № 4 (Тестирование) Тест №5 (Тестирование) Тест №6 (Тестирование)
ОПК-7	ОПК-7(Компетенция)	Знать: физические явления и процессы, применяемые для обеспечения информационной	Тест № 1; Тест № 2 (Тестирование) Тест № 3; Тест № 4 (Тестирование) Тест №5 (Тестирование) Тест №6 (Тестирование)

		безопасности объекта защиты Уметь: анализировать физические явления и процессы, применяемые для обеспечения информационной безопасности объекта защиты	

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. Тест № 1; Тест № 2

Формы реализации: Проверка задания
Тип контрольного мероприятия: Тестирование
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Всего вопросов -20 или 40. На вопросы задания даётся по 1 минуте. После проведения тестирования проводится проверка правильности ответов на вопросы и разбор типичных ошибок.

Краткое содержание задания:
Тест содержит вопросы **двух уровней сложности**. Вопросы повышенного уровня сложности отмечены звездочкой **(*).**
Тест состоит из **20 или 40** вопросов. При этом как в вопросах, так и в ответах учтена возможность **многовариантности решений.**
Вопросы, предлагающие выбрать **все верные варианты ответа,** имеют от **2** до **4** правильных вариантов ответа. Остальные вопросы имеют единственный правильный вариант ответа.
Ответ на вопрос считается **правильным,** если он является **полным.**
Во время тестирования запрещается:

- - пользоваться какой-либо литературой или заранее подготовленными записями;
- - разговаривать с другими тестируемыми;
- - мешать каким-либо способом другим тестируемым;
- - задавать преподавателю вопросы, не относящиеся к процедуре тестирования.

Контрольные вопросы/задания:

Знать: физические явления и процессы, применяемые для обеспечения информационной безопасности объекта защиты	1.Понятие концепции и политики безопасности при обеспечении ЗИ
Уметь: анализировать физические явления и процессы, применяемые для обеспечения информационной безопасности объекта защиты	1.Модель угроз - это 2.Какой документ ФСТЭК необходимо применять при обосновании актуальных угроз безопасности информации 3.Какой международный стандарт описывает менеджмент рисков ИБ

Описание шкалы оценивания:

Оценка: зачтено
Описание характеристики выполнения знания: Оценка "зачтено" выставляется если задание выполнено правильно или с незначительными недочетами

Оценка: не зачтено
Описание характеристики выполнения знания: Оценка "не зачтено" выставляется если задание не выполнено в отведенный срок или результат не соответствует заданию

КМ-2. Тест № 3; Тест № 4

Формы реализации: Билеты (письменный опрос)

Тип контрольного мероприятия: Тестирование
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Всего вопросов -20 или 40. На вопросы задания даётся по 1 минуте. После проведения тестирования проводится проверка правильности ответов на вопросы и разбор типичных ошибок.

Краткое содержание задания:

Тест содержит вопросы двух уровней сложности. Вопросы повышенного уровня сложности отмечены звездочкой (*).
Тест состоит из 20 или 40 вопросов. При этом как в вопросах, так и в ответах учтена возможность многовариантности решений.
Вопросы, предлагающие выбрать все верные варианты ответа, имеют от 2 до 4 правильных вариантов ответа. Остальные вопросы имеют единственный правильный вариант ответа.
Ответ на вопрос считается правильным, если он является полным.
Во время тестирования запрещается:

- - пользоваться какой-либо литературой или заранее подготовленными записями;
- - разговаривать с другими тестируемыми;
- - мешать каким-либо способом другим тестируемым;
- - задавать преподавателю вопросы, не относящиеся к процедуре тестирования.

Контрольные вопросы/задания:

Знать: анализировать физические явления и процессы, применяемые для обеспечения информационной безопасности объекта защиты	1.Существуют следующие стратегии обработки риска 2.Модель Шухарта-Деминга состоит из следующих этапов 3.Для поддержания уровня безопасности на должном уровне руководство обязано
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.Организации службы ИБ. Подразделение по ЗИ и его основные функции 2.Политика информационной безопасности хозяйствующего субъекта
Уметь: анализировать физические явления и процессы, применяемые для обеспечения информационной безопасности объекта защиты	1.Понятие критических информационных инфраструктур (КИИ) РФ

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. Тест №5

Формы реализации: Билеты (письменный опрос)
Тип контрольного мероприятия: Тестирование
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Всего вопросов -20 или 40. На вопросы задания даётся по 1 минуте. После проведения тестирования проводится проверка правильности ответов на вопросы и разбор типичных ошибок.

Краткое содержание задания:
Тест содержит вопросы двух уровней сложности. Вопросы повышенного уровня сложности отмечены звездочкой (*).
Тест состоит из 20 или 40 вопросов. При этом как в вопросах, так и в ответах учтена возможность многовариантности решений.
Вопросы, предлагающие выбрать все верные варианты ответа, имеют от 2 до 4 правильных вариантов ответа. Остальные вопросы имеют единственный правильный вариант ответа.
Ответ на вопрос считается правильным, если он является полным.
Во время тестирования запрещается:

- - пользоваться какой-либо литературой или заранее подготовленными записями;
- - разговаривать с другими тестируемыми;
- - мешать каким-либо способом другим тестируемым;
- - задавать преподавателю вопросы, не относящиеся к процедуре тестирования.

Контрольные вопросы/задания:

Знать: анализировать физические явления и процессы, применяемые для обеспечения информационной безопасности объекта защиты	1.Информационная система- это
Знать: физические явления и процессы, применяемые для обеспечения информационной безопасности объекта защиты	1.Составляющими угрозы являются 2.Предоставление информации - это
Уметь: анализировать физические явления и процессы, применяемые для обеспечения информационной безопасности объекта защиты	1.В соответствии с требованиями 152-ФЗ «О персональных данных», оператор, являющийся юридическим лицом, назначает 2.Реализация технического канала утечки информации может привести к нарушениям 3.Количество категорий внутренних нарушителей, определяемых нормативными документами ФСТЭК

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. Тест №6

Формы реализации: Билеты (письменный опрос)
Тип контрольного мероприятия: Тестирование
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Всего вопросов -20 или 40. На вопросы задания даётся по 1 минуте. После проведения тестирования проводится проверка правильности ответов на вопросы и разбор типичных ошибок.

Краткое содержание задания:
Тест содержит вопросы двух уровней сложности. Вопросы повышенного уровня сложности отмечены звездочкой (*).
Тест состоит из 20 или 40 вопросов. При этом как в вопросах, так и в ответах учтена возможность многовариантности решений.
Вопросы, предлагающие выбрать все верные варианты ответа, имеют от 2 до 4 правильных вариантов ответа. Остальные вопросы имеют единственный правильный вариант ответа.
Ответ на вопрос считается правильным, если он является полным.
Во время тестирования запрещается:

- - пользоваться какой-либо литературой или заранее подготовленными записями;
- - разговаривать с другими тестируемыми;
- - мешать каким-либо способом другим тестируемым;
- - задавать преподавателю вопросы, не относящиеся к процедуре тестирования.

Контрольные вопросы/задания:

Знать: анализировать физические явления и процессы, применяемые для обеспечения информационной безопасности объекта защиты	1.Сопротивления заземляющих проводников, а также земляных шин должны быть 2.По признаку отношений к природе возникновения угрозы классифицируются как
Знать: физические явления и процессы, применяемые для обеспечения информационной безопасности объекта защиты	1.Дайте определение понятию “информационная безопасность”
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.Несанкционированный доступ к информации может быть осуществлён путём 2.Требования к защите персональных данных при их обработке в информационных системах персональных данных определяются 3.К угрозам непосредственного доступа в операционную среду компьютера, реализуемым в ходе загрузки операционной системы, относятся

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

1 семестр

Форма промежуточной аттестации: Экзамен

Пример билета

1. Какой номер имеет основной (базовый) закон РФ в области ИБ?
1. 152
2. 63
3. 149
4. 187

Процедура проведения

Проводится экзамен на основе письменного тестирования по 45 вопросам, из которых 5 вопросов должны быть изложены письменно. На ответы по экзамену даётся 60 минут. После проверки ответов выставляются оценки, при необходимости задаются дополнительные вопросы для ответа устно.

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

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

Вопросы, задания

1.

1. Какой номер имеет основной (базовый) закон РФ в области ИБ?
1. 152
2. 63
3. 149
4. 187

45. Какой номер имеет ФЗ «О персональных данных»?
1. 188
2. 149
3. 152
4. 214

2.**3. Какой вид тайны информации не является профессиональной?**
1. Нотариальная
2. Коммерческая
3. Врачебная
4. Усыновления
5. Исповеди

3.**4. Какими минимальными свойствами должна обладать компьютерная программа, чтобы называться вирусом?**
1. Способностью проникать в компьютерные системы
2. Наносить вред компьютеру
3. Создавать свои копии
4. Сообщать о своём присутствии
5. 1,3

6. 1 - 4

4.**5. Какого типа антивирусного ПО не существует?**

1. Вакцины
2. Ревизоры
3. Детекторы
4. Доктора
5. Фаги
6. Все существуют

5.**7. От чего не должны зависеть требования безопасности к информационной системе?**

1. Назначение системы
2. Тип возможных угроз безопасности
3. Характер используемой информации
4. Решение руководителя (системного администратора)

6.**11. Какие требования к СОИБ, обусловленные характером информации, обрабатываемой в ИС, не предъявляются?**

1. Интенсивность обработки информации
2. Объёмы обрабатываемой информации
3. Степень конфиденциальности информации
4. Скорость обработки информации

7.**15. В формуле вычисления ТСО = Пр + Кр1 + Кр2, Кр - это**

1. Конечные ресурсы
2. Количественные риски
3. Косвенные расходы
4. Критериальные расчёты

8.**16. Средства охранного телевидения обеспечивают функционирование этой подсистемы**

1. Предупреждения угроз
2. Обозначения угроз
3. Обнаружения угроз
4. Ликвидации угроз

9.**18. Какое из перечисленных не является программным средством защиты информации, встроенным в ОС?**

1. Средства аутентификации
2. Средства анализа защищённости
3. Средства межсетевого экранирования
4. Средства резервного копирования
5. Средства аудита

10.**19. Какой процесс не является основным информационным процессом?**

1. Передача информации
2. Хранение информации
3. Уничтожение информации
4. Архивация информации
5. Сбор информации
6. Обработка информации
7. Использование информации

11.**25. Информация в зависимости от категории доступа к ней подразделяется на:**

1. Конфиденциальную
2. Общедоступную
3. Особо конфиденциальную
4. Ограниченного доступа

5. Широкого доступа
6. 2,4
7. 1-5

12.**26. В соответствии с законодательством РФ, информация - это**

1. Совокупность содержащихся в базах данных сведений
2. Совокупность содержащихся в базах данных сведений, зафиксированных на машинных носителях
3. Сведения (сообщения, данные) воспроизводимые различными системами
4. Сведения (сообщения, данные) независимо от формы их представления

13.**29. Информационная система - это**

1. Совокупность информации, информационных технологий и технических средств
2. Совокупность информации, информационных технологий и технических средств, и персонала, обслуживающего систему
3. Совокупность информационных технологий и технических средств
4. Совокупность информации, технических средств и персонала, обслуживающего систему

14.**31. Какого направления в кадровом обеспечении СОИБ не выделяется?**

1. Лицензирование и сертификация
2. Подготовка
3. Подбор
4. Профессиональная этика

15.**32. Какое направление деятельности не входит в подсистему инженерно-технического обеспечения ИБ?**

1. Инженерно-техническая защита территорий и помещений
2. Обнаружение и защита технических каналов утечки информации
3. Противопожарная защита объектов

16.**33. Связь между количеством информации и числом состояний системы определяется по формуле**

1. Келдыша
2. Берга
3. Хартли
4. Шеннона

17.**37. Какое направление деятельности не входит в подсистему инженерно-технического обеспечения ИБ?**

1. Инженерно-техническая защита территорий и помещений
2. Обнаружение и защита технических каналов утечки информации
3. Видеонаблюдение на объектах

18.**43. Регулирование деятельности в сфере шифровальных (криптографических) средств осуществляет**

1. ФСТЭК
2. ФСБ
3. Роскомнадзор
4. Ростехнадзор

19.**45. Какой номер имеет ФЗ «О персональных данных»?**

1. 188
2. 149
3. 152
4. 214

Материалы для проверки остаточных знаний

1.Какое действие не свойственно режиму конфиденциальности информации?

Ответы:

1. Ограничение доступа к информации
2. Порядок введения и прекращения
3. Степень жёсткости
4. Последствия нарушения

Верный ответ: 3

2.Какой гриф можно использовать для обозначения коммерческой тайны?

Ответы:

1. Конфиденциально
2. Особо ценная информация
4. Строго конфиденциально
5. Все приведённые

Верный ответ: 5

3.Какого уровня декомпозиции СОИБ не предполагается?

Ответы:

1. Подсистема
2. Средства
3. Направление
4. Обеспечение
5. Силы

Верный ответ: 4

4.Средства охранного телевидения обеспечивают функционирование этой подсистемы

Ответы:

1. Предупреждения угроз
2. Обозначения угроз
3. Обнаружения угроз
4. Ликвидации угроз

Верный ответ: 3

5.Какой уровень декомпозиции сложных систем не предусматривается?

Ответы:

1. Элемент системы
2. Подсистема
3. Составная часть системы

Верный ответ: 3

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

Вопросы, задания

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

1. Достоверность
2. Целостность
3. Конфиденциальность
4. Доступность
5. 1-3
6. 2-4

2.**6. Какие методы антивирусной защиты относятся к проактивным?**

1. Сигнатурные
2. Поведенческий блокиратор
3. Эвристические
4. 1-3
5. 1,3

3.**8. Какого вида обеспечения СОИБ не предусматривается?**

1. Организационно-правовое
2. Информационное
3. Программно-аппаратное
4. Кадровое
5. Аудита ИБ

4.**9. Главная цель СОИБ ХС - это**

1. Обеспечение устойчивого функционирования объекта защиты
2. Обеспечение устойчивого функционирования системы ИБ
3. Обеспечение устойчивого функционирования СЗИ

5.**10. Дайте определение понятия «Информационная безопасность»**

6.**12. Какого уровня декомпозиции СОИБ не предполагается?**

1. Подсистема
2. Средства
3. Направление
4. Обеспечение
5. Силы

7.**13. Какое действие не свойственно режиму конфиденциальности информации?**

1. Ограничение доступа к информации
2. Порядок введения и прекращения
3. Степень жёсткости
4. Последствия нарушения
5. Сроки действия

8.**14. Какой гриф можно использовать для обозначения коммерческой тайны?**

1. Коммерческая тайна
2. Конфиденциально
3. Особо ценная информация
4. Строго конфиденциально
5. Все приведённые

9.**17**. **Одним из основных условий успешности реализации угроз доступа к ресурсам и сервисам компьютера является:**

1. Удалённый доступ нарушителя к компьютеру
2. Физический доступ нарушителя к компьютеру
3. Наличие сетевого сканера
4. Физический доступ в помещение с компьютером

10.**20. Какая задача не свойственна для СОИБ организации?**

1. Обнаружение воздействия угроз
2. Ликвидация угроз
3. Ликвидация последствий воздействия угроз
4. Предупреждение угроз
5. Обнаружение угроз

11.**21. Какой уровень декомпозиции сложных систем не предусматривается?**

1. Элемент системы
2. Подсистема
3. Составная часть системы
4. Система

12.**22. Дайте определение целостности**

13.**23. Главная цель СОИБ ХС - это**

1. Обеспечение устойчивого функционирования объекта защиты
2. Обеспечение устойчивого функционирования системы ИБ
3. Обеспечение устойчивого функционирования СЗИ

14.**24. В понятие «государственная тайна» входит информация о…деятельности**

1. Контрразведывательной
2. Разведывательной
3. Военной
4. Внешнеполитической
5. Экономической
6. Оперативно-розыскной
7. 1 – 6
8. 1-4,6

15.**27. Угроза безопасности информации - это**

1. Условия и факторы, определяющие степень важности информации
2. Условия и факторы, определяющие опасность возникновения инцидента
3. Условия и факторы, определяющие опасность возникновения инцидента, который может привести к нанесению ущерба

16.**28. Уязвимость информационной системы это**

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

17.30. Дайте определение конфиденциальности

18.**34. Анализ чего предполагает декомпозиция 1-го уровня?**

1. Сложная система
2. Система
3. Подсистема
4. Элемент

19.**35. Какая подсистема не выделяется в СОИБ организации?**

1. Аудита ИБ
2. Инженерно - технического обеспечения
3. Финансово - экономического обеспечения
4. Кадрового обеспечения
5. Криптографического обеспечения

20.**36. Какие средства не относятся к средствам организационной защиты информации?**

1. Политика ИБ
2. Режим ИБ
3. Правила внутреннего распорядка дня
4. Федеральный Закон
5. Инструкция

21.**38. В подсистему инженерно – технического обеспечения ХС входят направления**

1. Инженерная защита
2. Физическая защита
3. Техническая защита
4. Обнаружение ТКУИ
5. Защита ТКУИ
6. Мероприятия по маскировке
7. 1-6
8. 1, 3-5

22.**39. Управление СОИБ ХС заключается в**

1. Манипуляции ресурсами
2. Целенаправленном воздействии на объект управления
3. Целенаправленном воздействии на субъект управления
4. Грамотных инвестициях в бизнес
5. Организации финансово - счётного подхода

23.40. Дайте определение доступности информации

24.**41. Источниками угроз безопасности информации являются**

1. Материальный объект
2. Элемент случайности
3. Субъект
4. Физическое явление
5. 1-4
6. 1,3,4

25.**42. Термин ОТСС в соответствии с нормативно - методическими документами ФСТЭК означает**

1. Особые технические средства и системы
2. Обычные технические средства и системы
3. Основные технические средства и системы

26.**44. Реализация технического канала утечки информации может привести к нарушению**

1. Конфиденциальности
2. Доступности
3. Целостности
4. Аутентичности

Материалы для проверки остаточных знаний

1.В формуле вычисления ТСО = Пр + Кр1 + Кр2, Кр - это

Ответы:

1. Конечные ресурсы
2. Количественные риски
3. Косвенные расходы
4. Критериальные расчёты

Верный ответ: 3

2.Одним из основных условий успешности реализации угроз доступа к ресурсам и сервисам компьютера является

Ответы:

1.Удалённый доступ нарушителя к компьютеру
2.Физический доступ нарушителя к компьютеру
3.Наличие сетевого сканера
4.Физический доступ в помещение с компьютером

Верный ответ: 4

3.Какое из перечисленных не является программным средством защиты информации, встроенным в ОС

Ответы:

1. Средства аутентификации
2. Средства анализа защищённости
3. Средства межсетевого экранирования
4. Средства резервного копирования
5. Средства аудита

Верный ответ: 2

4.Какой процесс не является основным информационным процессом?

Ответы:

1. 1. Передача информации
2. 2. Хранение информации
3. 3. Уничтожение информации
4. 4. Передача информации
5. 5. Архивация информации
6. 6. Сбор информации
7. 7. Обработка информации
8. 8. Использование информации

Верный ответ: 5

5.Какая задача не свойственна для СОИБ организации

Ответы:

1. Обнаружение воздействия угроз
2. Ликвидация угроз
3. Ликвидация последствий воздействия угроз
4. Предупреждение угроз
5. Обнаружение угроз

Верный ответ: 2

II. Описание шкалы оценивания

Оценка: 5
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: Работа выполнена в рамках "продвинутого" уровня. В ответе допущено не более 10 % ошибок, четко сформулированы особенности практических решений

Оценка: 4
Нижний порог выполнения задания в процентах: 75
Описание характеристики выполнения знания: Работа выполнена в рамках "базового" уровня. Большинство ответов даны верно. В ответе допущено не более 25 % ошибок.

Оценка: 3
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Работа выполнена в рамках "порогового" уровня. Основная часть задания выполнена верно. В ответе допущено не более 40 % ошибок.

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 (экзамена, проводимого по билетам).