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: ЭТАЛОН: информационная безопасность

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: Невский А.Ю. Идентификатор: R4bc65573-NevskyAY-0b6e493d	А.Ю. Невский
(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 способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства

ИД-1 Понимает значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации

ИД-2 Понимает значение информационной безопасности для обеспечения объективных потребностей личности, общества и государства

2. ОПК-6 способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю

ИД-2 Участвует в работах по реализации политики информационной безопасности, применяет комплексный подход к обеспечению информационной безопасности объекта защиты

и включает:

для текущего контроля успеваемости:

Форма реализации: Выполнение задания

1. Индивидуальное практическое задание № 1. Анализ общедоступной базы уязвимостей (Домашнее задание)
2. Индивидуальное практическое задание № 2. Разработка «Модели угроз безопасности информации организации «Х». (Домашнее задание)
3. Практическое задание № 1. Оценка ценности информации на основе анализа рисков информационной безопасности. (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)

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. Виды Политик 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:	30	20	30	20

$Общая часть/Для промежуточной аттестации$

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	ИД-1$_{ОПК-1}$ Понимает значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	Знать: критерии мотивации к выполнению профессиональной деятельности Уметь: выполнять профессиональную деятельность в области обеспечения информационной безопасности понимать социальную значимость своей будущей профессии	Практическое задание № 1. Оценка ценности информации на основе анализа рисков информационной безопасности. (Отчет) Практическое задание № 5. Анализ РД ФСТЭК «Концепция защиты средств вычислительной техники и автоматизированных систем от НСД к информации» (Доклад)
ОПК-1	ИД-2$_{ОПК-1}$ Понимает значение информационной безопасности для обеспечения объективных потребностей личности, общества и государства	Знать: состав и перечень защищаемой информации, классификацию ее по видам тайны информации, носителям информации, а также угрозы и уязвимости и возможные пути их реализации	Индивидуальное практическое задание № 1. Анализ общедоступной базы уязвимостей (Домашнее задание)
ОПК-6	ИД-2$_{ОПК-6}$ Участвует в	Знать:	Индивидуальное практическое задание № 2. Разработка «Модели угроз

	работах по реализации политики информационной безопасности, применяет комплексный подход к обеспечению информационной безопасности объекта защиты	источники, способы и результаты дестабилизирующего воздействия на защищаемую информацию Уметь: применять теоретические знания в области информационной безопасности на основе системного анализа и системного подхода	безопасности информации организации «Х». (Домашнее задание)

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. Индивидуальное практическое задание № 1. Анализ общедоступной базы уязвимостей

Формы реализации: Выполнение задания
Тип контрольного мероприятия: Домашнее задание
Вес контрольного мероприятия в БРС: 30
Процедура проведения контрольного мероприятия: Самостоятельное выполнение практического занятия.

Краткое содержание задания:
Используя материалы лекции по теме 3 и интернет - ресурсы провести анализ одной из общедоступных баз уязвимостей, относящихся к ИБ, поддерживаемых различными профильными организациями и вендорами.

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.Понятие уязвимости и природа (причины) возникновения уязвимостей в ИС. 2. Классификация уязвимостей по типу, привести примеры. 3. Классификация уязвимостей по компоненту, содержащему уязвимость, привести примеры. 4. Классификация уязвимостей по этапам жизненного цикла. 5. Классификация уязвимостей по преднамеренности внесения. Классификация уязвимостей по месту уязвимости в ИС

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. Оценка ценности информации на основе анализа рисков информационной безопасности.

Формы реализации: Выполнение задания

Тип контрольного мероприятия: Отчет
Вес контрольного мероприятия в БРС: 20
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.
Уметь: понимать социальную значимость своей будущей профессии	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

КМ-3. Индивидуальное практическое задание № 2. Разработка «Модели угроз безопасности информации организации «Х».

Формы реализации: Выполнение задания
Тип контрольного мероприятия: Домашнее задание
Вес контрольного мероприятия в БРС: 30
Процедура проведения контрольного мероприятия: Самостоятельное выполнение практического занятия.

Краткое содержание задания:
Используя материалы лекции по темам 2-5, методики определения угроз безопасности информации в информационных системах (проект 2015), методики определения угроз безопасности персональным данным (сайт ФСТЭК) и рекомендованные общедоступные интернет – ресурсы, разработать «Модель угроз безопасности информации организации «Х».

Контрольные вопросы/задания:

Знать: источники, способы и результаты дестабилизирующего	1.1.Модель угроз: понятие, цель разработки, выполняемые задачи.

воздействия на защищаемую информацию	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. 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-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: 20
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:

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: Экзамен

Пример билета

НИУ МЭИ	**ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №1** Кафедра: *Безопасности и информационных технологий* Дисциплина: «Теория информационной безопасности»	*Утверждаю:* *Зав. каф. БИТ* *А.Ю.Невский* *Протокол кафедры №* *« » декабря 2021г.*
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$_{ОПК-1}$ Понимает значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации

Вопросы, задания

1.1. Понятие ценности информации, свойства информации, определяющие ее ценность.

2.2. Методы определения ценности информации (личной, корпоративной и государственной).

3.6. Понятие угрозы безопасности информации.

4.29. Понятие и сущность Политики безопасности. Дуализм политики.

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

2. Компетенция/Индикатор: ИД-2$_{ОПК-1}$ Понимает значение информационной безопасности для обеспечения объективных потребностей личности, общества и государства

Вопросы, задания

1.3. Понятие тайны информации и современное состояние тайны информации в РФ.
2.7. Понятие угрозы безопасности информации. Основы классификации угроз.
3.8. Классификация угроз по характеру воздействия, расположению источника угроз, составляющим ИБ, составляющим ИБ.
4.10. Понятие уязвимости и природа (причины) возникновения уязвимостей в ИС.
5.11. Классификация уязвимостей по типу, компоненту содержащему уязвимость, этапам жизненного цикла, преднамеренности внесения, месту в ИС.
6.13. Понятие нарушителя и классификационные признаки нарушителей ИБ.
7.14. Общая характеристика внутренних и внешних нарушителей.
8.16. Характеристика основных групп нарушителей
9.37. Проблемы развития теории и практики обеспечения информационной безопасности
10.38. Интерпретация понятия информационной безопасности

Материалы для проверки остаточных знаний

1**.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

2**.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

3**.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

4**.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

5.**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

6.**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

7.**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

3. Компетенция/Индикатор: ИД-2$_{ОПК-6}$ Участвует в работах по реализации политики информационной безопасности, применяет комплексный подход к обеспечению информационной безопасности объекта защиты

Вопросы, задания

1.5. Информация ограниченного доступа. Несанкционированный доступ к информации.
2.9. Моделирование и разработка модели угроз
3.12. Основные понятие, назначение и работа с базами уязвимостей.
4.19. Системный подход к моделированию угроз безопасности информации.
5.21. Последовательность работ по моделированию угроз
6.22. Содержание «Модели угроз безопасности информации организации»
7.23. Оценка вероятности (возможности) реализации угроз безопасности информации
8.24. Оценка степени возможного ущерба от реализации угрозы безопасности информации
9.25. Определение актуальности угрозы безопасности информации

Материалы для проверки остаточных знаний

1.**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

2**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

3**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.

4**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

5**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

6**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

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

Ответы:

1. Сертифицированная

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

Верный ответ: 1

8.**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

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

Ответы:

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

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

III. Правила выставления итоговой оценки по курсу