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
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-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: Выполнение задания

1. Моделирование действий нарушителя информационной безопасности (Домашнее задание)
2. Моделирование систем контроля конфиденциальности информации (Расчетно-графическая работа)
3. Системный подход к моделированию угроз безопасности информации (Проверочная работа)
4. Уязвимости информационных (автоматизированных) систем (Домашнее задание)

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 лекция	+			
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). Постановка задачи моделирования.			+	
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: состав и перечень защищаемой информации, классификацию ее по видам тайны информации, носителям информации, а также угрозы и уязвимости и возможные пути их реализации	Уязвимости информационных (автоматизированных) систем (Домашнее задание)
ПК-4	ПК-4(Компетенция)	Знать: источники, способы и результаты дестабилизирующего воздействия на защищаемую информацию Уметь: применять теоретические знания в области информационной безопасности на основе системного анализа и системного подхода	Моделирование действий нарушителя информационной безопасности (Домашнее задание) Системный подход к моделированию угроз безопасности информации (Проверочная работа)
ПК-15	ПК-15(Компетенция)	Знать: нормативные методические документы	Уязвимости информационных (автоматизированных) систем (Домашнее задание) Моделирование систем контроля конфиденциальности информации

		федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области Уметь: формировать различные модели контроля конфиденциальности и целостности	(Расчетно-графическая работа)
ОК-5	ОК-5(Компетенция)	Знать: критерии мотивации к выполнению профессиональной деятельности Уметь: выполнять профессиональную деятельность в области обеспечения информационной безопасности	Системный подход к моделированию угроз безопасности информации (Проверочная работа)

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. Уязвимости информационных (автоматизированных) систем

Формы реализации: Выполнение задания
Тип контрольного мероприятия: Домашнее задание
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Задание выполняется самостоятельно в письменном виде к сроку, указанному в задании

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.

Исходные данные:

а) Выбор ресурса для исследования:

Примеры систем для выбора:

1. Компания MITRE и её база «Общие уязвимости и воздействия» (CommonVulnerabilitiesandExposures — CVE)
2. Национальный институт стандартов и технологий США (National Institute of Standards and Technology - NIST) и его Национальная база данных уязвимостей (National Vulnerabilities Database — NVD)
3. Открытая база данных уязвимостей» (OpenSource Vulnerability Database — OSVDB)
4. Группа чрезвычайного компьютерного реагирования США (United State Computer Emergency Readiness Team — US-CERT), база данных записей уязвимостей (Vulnerability Notes Database — VND)
5. Проект SecurityFocus, база уязвимостей BugTraq
6. Компания IBM, база уязвимостей X-Force
7. ФСТЭК России, база данных угроз (Раздел – уязвимости)
8. Лаборатория SecurityLab, база уязвимостей
9. Cisco Security Advisories and Responses, база уязвимостей
10. Software Engineering Institute, база уязвимостей
11. WPScan Vulnerability Database, база уязвимостей
12. Компания Secunia, база уязвимостей
13. VUPEN Security, база уязвимостей

б) Порядок представления результатов исследования

Работу оформить в **строгом** соответствии с ранее изученными требованиями к оформлению научных отчетов. Отчет должен содержать:

- **титульный лист:** (институт, домашнее задание, тема, кто выполнил, год) – 1 лист.
- **введение:** полное название, общая характеристика рассматриваемой системы, цель ее создания, выполняемые ею задачи и ее статус (открытая – закрытая, свободно распространяемая – коммерческая), объем – 1 лист);
- **основная часть**: Описание ресурса, его структура, основная целевая аудитория, перечень сведений о конкретной уязвимости, степень структурированности в базе, состояние ее актуальности, время последнего обновления, источники информации, удобство интерфейса, 2-3 скриншота основных возможностей (3-5 листов);
- **заключение:** краткие выводы о базе данных, ее возможностях, собственное суждение автора о преимуществах и недостатках ресурса (1лист).

Общий рекомендуемый объем – 6-8 листов.

в) Технология выполнения.

А) Номер базы угроз соответствует порядковому номеру студента в списке группы. Студент под номером 14 выбирает 1 вариант; 15 – 2 и т.д.
Б) Домашнее задание выполняется на компьютере в машинописной форме. Скриншоты, таблицы рассматриваемых ресурсов должны быть четкими и иметь возможность прочтения.

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.Для чего необходима информация об уязвимостях?
Знать: нормативные методические документы федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области	1.Каков перечень сведений об уязвимости в рассмотренном информационном ресурсе?

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Содержит полное и правильное описание .

Оценка: 4
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Содержит полное и правильное описание . При этом могут быть отдельные неточности

Оценка: 3
Нижний порог выполнения задания в процентах: 30
Описание характеристики выполнения знания: Выполнено в основном правильно, при этом даны описания , которые не обладают полнотой и имеют ошибки

КМ-2. Моделирование действий нарушителя информационной безопасности

Формы реализации: Выполнение задания
Тип контрольного мероприятия: Домашнее задание
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Задание выполняется самостоятельно в письменном виде к сроку, указанному в задании

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».
Исходные данные
а) Общие сведения об организации:
- ПАО «Сигма» занимается оптово-розничной продажей бытовой техники;

- виды конфиденциальной информации, обрабатываемой в ИС организации: коммерческая тайна, персональные данные сотрудников;
- общее количество персонала (штат) – 25 человек;
- режим КТ в организации установлен приказом ген. директора;
- обеспечение информационной безопасности в организации возложено на системного администратора ИС (нештатный сотрудник);
- перечень структурных подразделений и их состав: дирекция – 2 чел. (ген. директор и секретарь); организационный отдел – 2 чел. (руководитель и специалист); бухгалтерия – 4 чел. (гл. бухг., 2 бухг., спец. 1С); рекламный отдел – 3 чел. (руководитель и 2 специалиста); отдел продаж – 5 чел. (руководитель, 3 специалиста, спец. 1С); отдел маркетинга – 3 чел. (руководитель и 2 специалиста); склад – 6 чел. (заведующий, специалист 1С, кладовщик, рабочий – 2 чел., водитель);
- в организации в настоящее время работают 5 женщин (гл. бухг., 2 бухг., 2 специалиста отдела маркетинга и продаж);
- за 2019 год в ИС организации были зафиксированы 3 события, связанные с появлением в сторонних информационных системах сведений, являющихся ПДн сотрудников. Нарушитель режима ИБ – не установлен;
- принято решение о совершенствовании индивидуальной работы по профилактике нарушений ИБ;

б) Организационно- штатное расписание ПАО «Сигма»

Таблица 1

№ п п	Фамилия и инициалы	Должность	Семейное положение	Образование	Место жительства	Наличие судимости	Основные интересы	Особенности характера
1	2	3	4	5	6	7	8	9
1	Иванов И.И.	бухгалтер	холост	СПО	Москва	нет	Компьютерные игры	Вспыльчив

в) сведения о сотрудниках организации заполняются самостоятельно. Порядок заполнения таблицы 1:
- пункт 2 - см. образец;
- пункт 3 - должность из перечня структурных подразделений и их состава;
- пункт 4 - варианты заполнения: холост/женат (не замужем/замужем);
- пункт 5 - варианты заполнения: СО/СПО/ВО;
- пункт 6 – название города или др. населенного пункта;
- пункт 7 – варианты заполнения: да/нет;
- пункты 8 и 9 заполняются в произвольной форме.

3. Выполнить

а) предварительный этап:
- изучить сущность задания;
- заполнить таблицу 1;
- перечень данных таблицы (пункты 3 – 9) разбить на следующие категории относительно их отношения к определению потенциальной возможности нарушения ИБ: не имеющие значения/малозначимые/значимые;
- каждой категории сведений присвоить шкалу по следующим уровням значимости: для не имеющих значения 0 – 3; для малозначимых – 0 – 6; для значимых – 0 – 10;

Примечание: При этом таблица 2 может иметь вид, отличный от образца.
- конкретную оценку по пунктам 3 - 9 для каждого сотрудника определить самостоятельно и показать в таблице 2

Таблица 2

№ пп	Фамилия и инициалы	Категория 1			Категория 2		Категория 3		Сумма оценок
			Значение 1	Значение 2	…….			……	Значение n
1	2	3	4	5	6	7	8	9	10
1	Иванов И.И.	1	9	…….				7	36

- разработать цифровую интерпретацию психологического портрета потенциального нарушителя режима и правил ИБ в организации в диапазонах по значениям и категориям;
- создать автоматизированную систему расчета и оценки потенциальной предрасположенности сотрудников организации к нарушению режима и правил ИБ;
- разделить сотрудников, оценив их предрасположенность к нарушению режима правил ИБ, на категории: группа риска/общая группа;
- сделать общие выводы по работе, проведенной в области моделирования нарушителя.

4. Технология выполнения.
а) инструмент для выполнения задания студент определяет самостоятельно;
б) в качестве инструмента могут быть выбраны: офисные приложения: MS Excel, MS Visio, а также другие системы моделирования и разработки приложений;
в) для наглядности результатов должны быть предусмотрены возможности графического представления информации о сотрудниках, входящих в группу риска по конкретному (-ным) показателю (-ям), или акцентирование цветом, начертанием шрифта и др.;
г) в качестве графической интерпретации результатов рекомендуется использовать инструмент «лепестковая» диаграмма.

Контрольные вопросы/задания:

Знать: источники, способы и результаты дестабилизирующего воздействия на защищаемую информацию	1.Что включает современный психологический портрет нарушителя ИБ? 2.Каково назначение информационной системы поддержки практической работы по профилактике нарушений режима ИБ в организации?

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Содержит полное и правильное описание .

Оценка: 4
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Содержит полное и правильное описание . При этом могут быть отдельные неточности

Оценка: 3
Нижний порог выполнения задания в процентах: 30
Описание характеристики выполнения знания: Выполнено в основном правильно, при этом даны описания , которые не обладают полнотой и имеют ошибки

КМ-3. Моделирование систем контроля конфиденциальности информации

Формы реализации: Выполнение задания
Тип контрольного мероприятия: Расчетно-графическая работа
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Задание выполняется самостоятельно в письменном виде к сроку, указанному в задании

Краткое содержание задания:

4. Порядок представления результатов исследования
Работу оформить в **строгом** соответствии с ранее изученными требованиями к оформлению научных отчетов. Отчет должен содержать:
- титульный лист: (институт, практическое задание, тема, кто выполнил, год) – 1 лист.
- **введение:** Сущность задания, предмет исследования – 1 лист);
- **основная часть**: Перечень исходных данных и обоснование их состава и значений и условных обозначений. Матрица прав доступа и обоснование выполнения правил NRU и NWD (2 листа);
- **приложения:** условные обозначения основных элементов модели (1 лист).
Общий рекомендуемый объем – 5 листов.
5. Дополнительные сведения
Работа каждого студента должна обладать оригинальностью. **Одинаковых моделей быть не должно!**
Для оформления работы использовать учебное пособие «Методика выполнения выпускной квалификационной работы бакалавра».
По всем вопросам, возникающим при выполнении задания, обращаться к преподавателю учебной дисциплины «Теория информационной безопасности».

Контрольные вопросы/задания:

Уметь: формировать различные модели контроля конфиденциальности и целостности	1.Продемонстрировать выполнение основных правил модели БЛМ на матрице прав доступа

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Матрица прав доступа содержит полное и правильное описание.

Оценка: 4
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Матрица прав доступа содержит полное и правильное описание . При этом может быть ошибка в 1-2 случаях доступа "субъект - объект"

Оценка: 3
Нижний порог выполнения задания в процентах: 30
Описание характеристики выполнения знания: Матрица прав доступа содержит полное описание . При этом может быть ошибка, не более чем в 4 случаях доступа "субъект - объект"

КМ-4. Системный подход к моделированию угроз безопасности информации

Формы реализации: Выполнение задания
Тип контрольного мероприятия: Проверочная работа
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Практическое задание выполняется на учебном занятии в течение 1 учебного часа

Краткое содержание задания:

Используя документ «Методика определения актуальных угроз……», ознакомиться с его содержанием и проверить адекватность методики на оценке актуальности следующих угроз:
Угроза несанкционированного доступа к акустической и видовой информации в организации.
Угроза несанкционированного доступа к информации вследствие неправильных (ошибочных) действий пользователя.
Исходные данные
а) исходные данные, необходимые для расчетов по Методике определить самостоятельно
Материалы
Официальный сайт ФСТЭК России

Контрольные вопросы/задания:

Знать: критерии мотивации к выполнению профессиональной деятельности	1.Какие исходные данные необходимы для оценки актуальности угроз безопасности ПДн? 2.В каких единицах “измеряется” актуальность угроз безопасности ПДн?
Уметь: применять теоретические знания в области информационной безопасности на основе системного анализа и системного подхода	1.Как была построена процедура оценки актуальности угроз?
Уметь: выполнять профессиональную деятельность в области обеспечения информационной безопасности	1.С помощью какого приложения была выполнена оценка актуальности угроз?

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Содержит полное описание и правильную оценку актуальности угроз.

Оценка: 4
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Содержит полное описание и правильную оценку актуальности угроз. При этом могут быть отдельные неточности

Оценка: 3
Нижний порог выполнения задания в процентах: 30
Описание характеристики выполнения знания: Содержит полное описание. При оценке актуальности угроз допущены ошибки.

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:*** Зам. зав. кафедрой БИТ _____/*О.Р.Баронов*/ *Протокол заседания кафедры №* ____ *«___» _____ 20___ г.*
1. Понятие ценности информации. Шкалы ценности информации. Определение ценности информации с позиции прав доступа к ней. 2. Практическая значимость композиции BLM – BM. Порядок объединения моделей.		

Процедура проведения

Экзамен по дисциплине «Теория информационной безопасности» проводится в письменной форме по билетам. Выполняется в течение 50 минут В экзаменационном билете два теоретических вопроса.

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

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

Вопросы, задания

1.22. Практическая ценность информации об уязвимостях. Информационные источники данных об уязвимостях: назначение, базы уязвимостей, описание уязвимости.
2.26. Модель нарушителя: назначение, содержание, категорирование, характеристика.
3.27. Модель угроз безопасности информации организации. Понятие, назначение, содержание и последовательность разработки.
4.28. Политика (модель) безопасности информации: понятие, уровень формализации, виды, краткая характеристика и примеры.

Материалы для проверки остаточных знаний

1.6. 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

2.11. Дайте определение метода защиты информации
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;
4.16. 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
5.19. Каких видов моделей угроз безопасности информации не разрабатывается?
Ответы:
1. Сертифицированная
2. Базовая
3. Отраслевая
4. Частная
5. Типовая

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

Вопросы, задания

1.2. Общий контекст информационной безопасности в концепции менеджмента ИБ.
2.10. Понятие угрозы безопасности информации, необходимость и подходы к классификации угроз.
3.11. Классификация угроз безопасности информации по характеру воздействия. Перечень причин и мотивов возникновения угроз. Примеры угроз.
4.12. Классификация угроз безопасности информации по расположению источника угрозы. Причины возникновения угроз. Примеры угроз.
5.13. Классификация угроз безопасности информации по составляющим информационной безопасности. Причины возникновения угроз. Примеры угроз.
6.14. Классификация угроз безопасности информации по компонентам информационной (автоматизированной) системы. Причины возникновения угроз. Примеры угроз.
7.15. Информационные источники данных об угрозах. Базы угроз: назначение, примеры, описание.
8.16. Понятие уязвимости информации, причины возникновения уязвимостей, классификация уязвимостей.
9.17. Классификация по типу уязвимостей в информационной системе. Причины возникновения и примеры уязвимостей.
10.18. Классификация по месту уязвимостей в информационной системе. Причины возникновения и примеры уязвимостей.
11.19. Классификация уязвимостей по типу компонента информационной системы, содержащего уязвимость. Причины возникновения и примеры уязвимостей.
12.20. Классификация уязвимостей по этапам жизненного цикла информационной системы. Причины возникновения и примеры уязвимостей.

13.23. Классификация нарушителей информационной безопасности по их отношению к информационной системе. Причины возникновения и примеры нарушений.
14.24. Классификация нарушителей информационной безопасности по используемым ими методам и средствам. Причины возникновения и примеры нарушений.
15.25. Классификация нарушителей информационной безопасности по их уровню подготовки (знаний). Причины возникновения и примеры нарушений.
16.42. Понятие НСД к информации, причины НСД, варианты доступа к информации.
17.43. Методы НСД к информации и их краткая характеристика.
18.44. Методы организации работ по защите информации от НСД и их краткая характеристика.
19.45. Общая характеристика Государственной системы защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам.

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

2.10. Какое название не является видом политики безопасности?

Ответы:

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

3.12. 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

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

Вопросы, задания

1.3. Модель CIA. Актуальность модели CIA в современном информационном мире.
2.4. Актуальные проблемы информационной безопасности в Российской Федерации и их краткая характеристика.
3.6. Понятие ценности информации. Шкалы ценности информации. Определение ценности информации с позиции прав доступа к ней.
4.7. Понятие тайны информации, виды тайны информации, проблема классификации информации по видам тайны.
5.9. Понятие несанкционированного доступа к информации. Характеристика несанкционированного доступа как нарушения правил разграничения доступа.
6.21. Классификация уязвимостей в информационной системе по преднамеренности внесения. Причины возникновения и примеры уязвимостей.

7.29. Постановка и описание дискреционной модели HRU: название, назначение, исходные данные, допущения, доказательство безопасности.
8.30. Постановка и описание мандатной модели BLM: название, правила мандатной модели, исходные данные, графическая интерпретация модели.
9.32. Постановка и описание BM: название, правила модели, варианты модели, графическая интерпретация модели.
10.33. Практическая значимость BM, композиция вариантов реализации модели.
11.34. Практическая значимость композиции BLM – BM. Порядок объединения моделей.
12.40. Характеристика современного уровня регламентации требований по обеспечению безопасности защищаемой информации. Методы организации работ.

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

2.17. 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

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

Вопросы, задания

1.8. Организация доступа к информации с позиции взаимодействия субъектов информационных взаимоотношений. Законодательное регулирование доступа.
2.39. Особенности реализации мероприятий информационной безопасности для отдельных категорий защищаемой информации: информация в государственных информационных системах, персональные данные, критическая информационная инфраструктура.
3.41. Характеристика основных методов организации работ по защите информационных активов организации, их преимущества и недостатки.

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

2.4. 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

3.5. Сформулируйте цель разработки Модели угроз безопасности…

4.18. Дайте определение НСД к информации

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