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

Рабочая программа дисциплины
УПРАВЛЕНИЕ ИНЦИДЕНТАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Блок:	**Блок 1 «Дисциплины (модули)»**
Часть образовательной программы:	**Вариативная**
№ дисциплины по учебному плану:	**Б1.В.06**
Трудоемкость в зачетных единицах:	**8 семестр - 4;**
Часов (всего) по учебному плану:	**144 часа**
Лекции	**8 семестр - 28 часа;**
Практические занятия	**8 семестр - 28 часа;**
Лабораторные работы	**не предусмотрено учебным планом**
Консультации	**8 семестр - 2 часа;**
Самостоятельная работа	**8 семестр - 85,5 часа;**
в том числе на КП/КР	**не предусмотрено учебным планом**
Иная контактная работа	**проводится в рамках часов аудиторных занятий**
включая: **Тестирование** **Контрольная работа**	
Промежуточная аттестация:	
Экзамен	**8 семестр - 0,5 часа;**

Москва 2018

ПРОГРАММУ СОСТАВИЛ:

Преподаватель	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Писаренко И.В. Идентификатор: R2828e375-PisarenkoIV-105ccd67	И.В. Писаренко
(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)

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель освоения дисциплины: формирование системы знаний и практических навыков в области менеджмента инцидентов информационной безопасности, возникающих в ходе деятельности организации, связанных с проведением расследований по выявленным инцидентам.

Задачи дисциплины

- изучение теоретических основ менеджмента инцидентов информационной безопасности на предприятии (в организации);
- освоение основных способов и методов выявления инцидентов информационной безопасности и проведения расследований по выявленным инцидентам;
- приобретение практических навыков в проведении расследований инцидентов информационной безопасности.

Формируемые у обучающегося **компетенции** и запланированные **результаты обучения** по дисциплине, соотнесенные с **индикаторами достижения компетенций**:

Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**	**Запланированные результаты обучения**
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		знать: - направления и перспективы дальнейшего совершенствования систем обеспечения безопасности хозяйствующих субъектов. 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.
ПК-4 способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты		уметь: - выполнять работы по эксплуатации подсистем управления информационной безопасностью предприятия.
ПК-10 способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности		уметь: - проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов, разрабатывать предложения по совершенствованию системы управления информационной безопасностью.

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Запланированные результаты обучения
ПК-12 способностью принимать участие в проведении экспериментальных исследований системы защиты информации		уметь: - проводить экспериментальные исследования системы защиты информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к части, формируемой участниками образовательных отношений блока дисциплин основной профессиональной образовательной программе Безопасность компьютерных систем (далее – ОПОП), направления подготовки 10.03.01 Информационная безопасность, уровень образования: высшее образование - бакалавриат.

Базируется на уровне среднего общего образования.

Результаты обучения, полученные при освоении дисциплины, необходимы при выполнении выпускной квалификационной работы.

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единицы, 144 часа.

№ п/п	Разделы/темы дисциплины/формы промежуточной аттестации	Всего часов на раздел	Семестр	Распределение трудоемкости раздела (в часах) по видам учебной работы										Содержание самостоятельной работы/ методические указания
				Контактная работа								СР		
				Лек	Лаб	Пр	Консультация		ИКР		ПА	Работа в семестре	Подготовка к аттестации /контроль	
							КПР	ГК	ИККП	ТК				
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	Вводная лекция	8	8	2	-	2	-	-	-	-	-	4	-	***Подготовка к практическим занятиям:*** Изучение материала по разделу "Вводная лекция" подготовка к выполнению заданий на практических занятиях ***Подготовка к контрольной работе:*** Изучение материалов по разделу Вводная лекция и подготовка к контрольной работе ***Подготовка домашнего задания:*** Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Вводная лекция" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам. ***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы ***Подготовка к текущему контролю:*** Повторение материала по разделу "Вводная лекция" ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Вводная лекция"
1.1	Предмет и задачи курса.	8		2	-	2	-	-	-	-	-	4	-	

														Изучение материалов литературных источников: [1], 1-328 [3], 1-176
2	Управление инцидентами информационной безопасности	52		12	-	12	-	-	-	-	-	28	-	***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Управление инцидентами информационной безопасности" ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Управление инцидентами информационной безопасности" подготовка к выполнению заданий на практических занятиях ***Подготовка к контрольной работе:*** Изучение материалов по разделу Управление инцидентами информационной безопасности и подготовка к контрольной работе ***Подготовка домашнего задания:*** Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Управление инцидентами информационной безопасности" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам. ***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы ***Подготовка к текущему контролю:*** Повторение материала по разделу "Управление инцидентами информационной безопасности" ***Изучение материалов литературных источников:***
2.1	Тема 1. Общая характеристика инцидентов информационной безопасности	18		4	-	4	-	-	-	-	-	10	-	
2.2	Тема 2. Основные способы и методы выявления инцидентов информационной безопасности	18		4	-	4	-	-	-	-	-	10	-	
2.3	Тема 3. Управление инцидентами информационной безопасности.	16		4	-	4	-	-	-	-	-	8	-	

														[1], 1-328 [2], 1-256 [3], 1-176
3	Проведение расследований инцидентов информационной безопасности	48		14	-	14	-	-	-	-	-	20	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Проведение расследований инцидентов информационной безопасности" ***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Проведение расследований инцидентов информационной безопасности" ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Проведение расследований инцидентов информационной безопасности" подготовка к выполнению заданий на практических занятиях ***Подготовка к контрольной работе:*** Изучение материалов по разделу Проведение расследований инцидентов информационной безопасности и подготовка к контрольной работе ***Подготовка домашнего задания:*** Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Проведение расследований инцидентов информационной безопасности" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам. ***Изучение материалов литературных источников:***
3.1	Тема 4. Расследование инцидентов информационной безопасности	26		8	-	8	-	-	-	-	-	10	-	
3.2	Тема 5. Порядок действий при расследовании инцидентов информационной безопасности	22		6	-	6	-	-	-	-	-	10	-	

														[2], 1-256 [4], 1-208 [5], 130-141
	Экзамен	36.0		-	-	-	-	2	-	-	0.5	-	33.5	
	Всего за семестр	**144.0**		**28**	**-**	**28**	**-**	**2**	**-**	**-**	**0.5**	**52**	**33.5**	
	Итого за семестр	**144.0**		**28**	**-**	**28**	**2**		**-**		**0.5**	**85.5**		

Примечание: Лек – лекции; Лаб – лабораторные работы; Пр – практические занятия; КПР – аудиторные консультации по курсовым проектам/работам; ИККП – индивидуальные консультации по курсовым проектам/работам; ГК- групповые консультации по разделам дисциплины; СР – самостоятельная работа студента; ИКР – иная контактная работа; ТК – текущий контроль; ПА – промежуточная аттестация

3.2 Краткое содержание разделов

1. Вводная лекция

1.1. Предмет и задачи курса.

Значение и место курса в подготовке специалистов по защите информации. Взаимосвязь курса с другими дисциплинами. Роль и место системы менеджмента инцидентов информационной безопасности в обеспечении информационной безопасности хозяйствующего субъекта. Разделы и темы, их распределение по видам аудиторных занятий. Формы проведения семинарских занятий. Состав и методика самостоятельной работы студентов по изучению дисциплины. Формы проверки знаний. Компетенции студентов, которые должны быть сформированы в результате изучения курса..

2. Управление инцидентами информационной безопасности

2.1. Тема 1. Общая характеристика инцидентов информационной безопасности

Понятия события и инцидента информационной безопасности. Международные стандарты в области информационной безопасности и лучшие практики по управлению инцидентами информационной безопасности. Классификация инцидентов информационной безопасности. Критичность инцидентов информационной безопасности, место их возникновения, причины и источники инцидентов. Основные стадии развития инцидентов информационной безопасности. Примеры инцидентов информационной безопасности и возможные причины их возникновения. Возможные последствия инцидентов информационной безопасности. Понятие ущерба. Виды ущерба: прямой, косвенный, репутационный. Оценка ущерба от инцидента информационной безопасности. Основные предпосылки возникновения инцидентов информационной безопасности в организации. Категории нарушителей информационной безопасности: внутренние и внешние. Модель нарушителя информационной безопасности. Основные мотивы совершения инцидентов информационной безопасности..

2.2. Тема 2. Основные способы и методы выявления инцидентов информационной безопасности

Основные способы и методы выявления инцидентов информационной безопасности. Использование технических средств и способов выявления инцидентов информационной безопасности. Получение информации от администраторов и пользователей организации. Концепция и структура построения системы управления инцидентами информационной безопасности. Средства сбора и хранения информации. Особенности построения SOC (центра управления безопасностью), используемые технические средства управления инцидентами информационной безопасности. Анализ и приоритезация инцидентов информационной безопасности. Принятие решения о наступлении инцидента информационной безопасности. Оценка степени его критичности. Понятие мониторинга информационной безопасности, виды и средства мониторинга. Использование средств мониторинга информационной безопасности. Примеры технических реализаций систем мониторинга информационной безопасности..

2.3. Тема 3. Управление инцидентами информационной безопасности.

Понятие менеджмента инцидентов информационной безопасности. Этапы менеджмента инцидентов информационной безопасности. Подготовка и планирование системы менеджмента. Использование системы менеджмента. Анализ и совершенствование системы менеджмента инцидентов информационной безопасности. Создание группы расследования инцидентов информационной безопасности. Документация системы менеджмента инцидентов информационной безопасности. Извлечение уроков из инцидентов

информационной безопасности. Тенденции, проблемные области, выявляемые в ходе анализа инцидентов информационной безопасности. База инцидентов информационной безопасности. Формы сообщений об инцидентах информационной безопасности. Особенности практического использования системы менеджмента инцидентов информационной безопасности в организации..

3. Проведение расследований инцидентов информационной безопасности

3.1. Тема 4. Расследование инцидентов информационной безопасности

Понятие расследования инцидента информационной безопасности. Типовые ситуации, возникающие в ходе расследования инцидентов информационной безопасности. Возможности службы безопасности и правоохранительных органов по проведению расследований инцидентов информационной безопасности. Правовые основы проведения расследований инцидентов информационной безопасности, определяющие порядок и сроки проведения расследований по нарушениям трудовой дисциплины. Организация взаимодействия с правоохранительными органами. Негосударственные организации, занимающиеся расследованием инцидентов информационной безопасности на территории Российской Федерации, и их возможности..

3.2. Тема 5. Порядок действий при расследовании инцидентов информационной безопасности

Проведение расследований инцидентов информационной безопасности: назначение руководителя расследования, сбор свидетельств возникновения инцидентов, обеспечение их сохранности. Планирование расследования. Алгоритм действий работников группы реагирования при возникновении инцидентов информационной безопасности. Выявление нарушителя, установление причин и мотивов инцидента информационной безопасности, опрос нарушителя и свидетелей инцидента, сбор объяснений по факту инцидента информационной безопасности. Оформление документов по расследованию инцидента информационной безопасности. Привлечение нарушителя к дисциплинарной ответственности. Взаимодействие с юридической службой и руководителем нарушителя. Виды взысканий, порядок наложения и снятия дисциплинарного взыскания. Правовые основы для изъятия и исследования компьютерной техники. Методика изъятия компьютерной техники и носителей информации. Обеспечение доказательственного значения изъятых материалов. Методика исследования компьютерной техники. Выводы эксперта и экспертное заключение..

3.3. Темы практических занятий

1. 1.Основные предпосылки возникновения инцидентов информационной безопасности в организации;
2. 2.Категории нарушителей информационной безопасности: внутренние и внешние. Модель нарушителя информационной безопасности. Основные мотивы совершения инцидентов информационной безопасности;
3. 3.Технические средства выявления инцидентов информационной безопасности. Порядок их использования;
4. 4.Политика и программа менеджмента инцидентов информационной безопасности;
5. 5.Практическая работа по выявлению и расследованию инцидентов информационной безопасности;
6. 6.Практическая работа по планированию расследования инцидента информационной безопасности;
7. 7.Изъятие и исследование компьютерной техники и носителей информации. Обеспечение доказательственного значения изъятых материалов. Описание и

пломбирование техники;
8. 8.Методика исследования компьютерной техники. Общие принципы исследования техники. Техническое обеспечение исследования;
9. 9.Оформление инцидентов информационной безопасности. Ведение базы инцидентов информационной безопасности.

3.4. Темы лабораторных работ

не предусмотрено

3.5 Консультации

Текущий контроль (ТК)

1. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Вводная лекция"
2. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Управление инцидентами информационной безопасности"
3. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Проведение расследований инцидентов информационной безопасности"

3.6 Тематика курсовых проектов/курсовых работ

Курсовой проект/ работа не предусмотрены

3.7. Соответствие разделов дисциплины и формируемых в них компетенций

Запланированные результаты обучения по дисциплине (в соответствии с разделом 1)	Коды индикаторов	Номер раздела дисциплины (в соответствии с п.3.1)			Оценочное средство (тип и наименование)
		1	2	3	
Знать:					
направления и перспективы дальнейшего совершенствования систем обеспечения безопасности хозяйствующих субъектов	ОПК-7(Компетенция)	+			Контрольная работа/Контрольная работа № 1
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	ОПК-7(Компетенция)	+			Тестирование/Тест № 1
выполнять работы по эксплуатации подсистем управления информационной безопасностью предприятия	ПК-4(Компетенция)			+	Контрольная работа/Контрольная работа № 2
проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов, разрабатывать предложения по совершенствованию системы управления информационной безопасностью	ПК-10(Компетенция)		+	+	Контрольная работа/Контрольная работа № 2
проводить экспериментальные исследования системы защиты информации	ПК-12(Компетенция)		+		Тестирование/Тест № 2

4. КОМПЕТЕНТНОСТНО-ОРИЕНТИРОВАННЫЕ ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ КОНТРОЛЯ ОСВОЕНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (ТЕКУЩИЙ КОНТРОЛЬ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ПО ДИСЦИПЛИНЕ)

4.1. Текущий контроль успеваемости

8 семестр

Форма реализации: Письменная работа

1. Контрольная работа № 1 (Контрольная работа)
2. Контрольная работа № 2 (Контрольная работа)
3. Тест № 1 (Тестирование)
4. Тест № 2 (Тестирование)

Балльно-рейтинговая структура дисциплины является приложением А.

4.2 Промежуточная аттестация по дисциплине

Экзамен (Семестр №8)

Итоговая оценка выставляется по итогам экзамена, с учетом оценки за курсовую работу и оценок по текущей успеваемости.

В диплом выставляется оценка за 8 семестр.

Примечание: Оценочные материалы по дисциплине приведены в фонде оценочных материалов ОПОП.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1 Печатные и электронные издания:

1. Одинцов, А. А. Защита предпринимательства: Экономическая и информационная безопасность : Учебное пособие по специальностям "Менеджмент организации", "финансы и кредит", "Прикладная информатика в экономике" / А. А. Одинцов . – М. : Международные отношения, 2003 . – 328 с. - ISBN 5-7133-1169-4 .;
2. Организационно-правовое обеспечение информационной безопасности : учебное пособие для вузов по специальностям 090102 "Компьютерная безопасность", 090105 "Комплексное обеспечение информационной безопасности автоматизированных систем", 090106 "Информационная безопасность телекоммуникационных систем" / А. А. Стрельцов, [и др.] . – М. : АКАДЕМИЯ, 2008 . – 256 с. – (Высшее профессиональное образование) . - ISBN 978-5-7695-4240-4 .;
3. Анисимов, А. А. Менеджмент в сфере информационной безопасности : учебное пособие / А. А. Анисимов . – М. : БИНОМ. Лаборатория знаний : Интернет-Ун-т информ. технологий, 2010 . – 176 с. – (Основы информационных технологий) . - ISBN 978-5-9963-0237-6 .;
4. Галатенко, В.А. Основы информационной безопасности. Курс лекций : учебное пособие для вузов по специальностям в области информационных технологий / В.А. Галатенко ; Ред. В. Б. Бетелин . – 3-е изд . – М. : Интернет-Ун-т информ. технологий, 2006 . – 208 с. – (Основы информационных технологий) . - ISBN 5-9556005-2-3 .;
5. А. А. Анисимов- "Менеджмент в сфере информационной безопасности: курс лекций", Издательство: "Интернет-Университет Информационных Технологий (ИНТУИТ)|Бином. Лаборатория знаний", Москва, 2009 - (176 с.)
https://biblioclub.ru/index.php?page=book&id=232981.

5.2 Лицензионное и свободно распространяемое программное обеспечение:
1. СДО "Прометей";
2. Office / Российский пакет офисных программ;
3. Windows / Операционная система семейства Linux;
4. Майнд Видеоконференции.

5.3 Интернет-ресурсы, включая профессиональные базы данных и информационно-справочные системы:
1. **ЭБС Лань** - https://e.lanbook.com/
2. **ЭБС "Университетская библиотека онлайн"** - http://biblioclub.ru/index.php?page=main_ub_red
3. **База данных Web of Science** - http://webofscience.com/
4. **База данных Scopus** - http://www.scopus.com
5. **Национальная электронная библиотека** - https://rusneb.ru/
6. **ЭБС "Консультант студента"** - http://www.studentlibrary.ru/
7. **Журнал Science** - https://www.sciencemag.org/
8. **Электронная библиотека МЭИ (ЭБ МЭИ)** - http://elib.mpei.ru/login.php
9. **Информационно-справочная система «Кодекс/Техэксперт»** - Http:\\proinfosoft.ru; http://docs.cntd.ru/
10. **Открытая университетская информационная система «РОССИЯ»** - https://uisrussia.msu.ru

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Тип помещения	Номер аудитории, наименование	Оснащение
Учебные аудитории для проведения лекционных занятий и текущего контроля	К-601, Учебная аудитория	парта со скамьей, стол преподавателя, стул, трибуна, доска меловая, мультимедийный проектор, экран
	А-300, Учебная аудитория "А"	кресло рабочее, парта, стеллаж, стол преподавателя, стол учебный, стул, трибуна, микрофон, мультимедийный проектор, экран, доска маркерная, колонки, техническая аппаратура, кондиционер, телевизор
Учебные аудитории для проведения практических занятий, КР и КП	З-512, Учебная аудитория	парта, стол преподавателя, стул, доска меловая
Учебные аудитории для проведения промежуточной аттестации	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
	З-512, Учебная аудитория	парта, стол преподавателя, стул, доска меловая
Помещения для самостоятельной работы	НТБ-303, Компьютерный читальный зал	стол компьютерный, стул, стол письменный, вешалка для одежды, компьютерная сеть с выходом в Интернет, компьютер персональный, принтер, кондиционер
Помещения для консультирования	З-512, Учебная аудитория	парта, стол преподавателя, стул, доска меловая
Помещения для хранения оборудования и учебного	К-202/2, Склад кафедры БИТ	стеллаж для хранения инвентаря, стол, стул, шкаф для документов, шкаф для

инвентаря		хранения инвентаря, тумба, запасные комплектующие для оборудования

Приложение А

БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА ДИСЦИПЛИНЫ

Управление инцидентами информационной безопасности

(название дисциплины)

8 семестр

Перечень контрольных мероприятий <u>текущего контроля</u> успеваемости по дисциплине:
КМ-1 Тест № 1 (Тестирование)
КМ-2 Контрольная работа № 1 (Контрольная работа)
КМ-3 Тест № 2 (Тестирование)
КМ-4 Контрольная работа № 2 (Контрольная работа)

Вид промежуточной аттестации – Экзамен.

Номер раздела	Раздел дисциплины	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
		Неделя КМ:	4	8	12	15
1	Вводная лекция					
1.1	Предмет и задачи курса.		+	+		
2	Управление инцидентами информационной безопасности					
2.1	Тема 1. Общая характеристика инцидентов информационной безопасности				+	+
2.2	Тема 2. Основные способы и методы выявления инцидентов информационной безопасности				+	+
2.3	Тема 3. Управление инцидентами информационной безопасности.				+	+
3	Проведение расследований инцидентов информационной безопасности					
3.1	Тема 4. Расследование инцидентов информационной безопасности					+
3.2	Тема 5. Порядок действий при расследовании инцидентов информационной безопасности					+
Вес КМ, %:			25	25	25	25