Министерство науки и высшего образования РФ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Национальный исследовательский университет «МЭИ»

Направление подготовки/специальность: 10.03.01 Информационная безопасность

Наименование образовательной программы: Безопасность автоматизированных систем

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очно-заочная

Рабочая программа дисциплины
УПРАВЛЕНИЕ ИНЦИДЕНТАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Блок:	**Блок 1 «Дисциплины (модули)»**
Часть образовательной программы:	**Часть, формируемая участниками образовательных отношений**
№ дисциплины по учебному плану:	**Б1.Ч.06**
Трудоемкость в зачетных единицах:	**10 семестр - 4;**
Часов (всего) по учебному плану:	**144 часа**
Лекции	**10 семестр - 16 часов;**
Практические занятия	**10 семестр - 20 часов;**
Лабораторные работы	**не предусмотрено учебным планом**
Консультации	**10 семестр - 2 часа;**
Самостоятельная работа	**10 семестр - 105,5 часов;**
в том числе на КП/КР	**не предусмотрено учебным планом**
Иная контактная работа	**проводится в рамках часов аудиторных занятий**
включая: **Тестирование** **Контрольная работа** **Коллоквиум**	
Промежуточная аттестация:	
Экзамен	**10 семестр - 0,5 часа;**

Москва 2023

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
ПК-1 Готов обеспечивать защиту информации в автоматизированных системах в процессе их эксплуатации	ПК-1.4$_{ПК-1}$ Выполняет аудит защищенности информации в автоматизированных системах	знать: - требования нормативных и правовых документов (законы, стандарты, регламенты) в предметной области дисциплины;; - основы управления инцидентами информационной безопасности на предприятии;; - особенности управления инцидентами информационной безопасности применительно к различным сферам деятельности.. уметь: - определять основные виды угроз информационной безопасности, возможные методы и пути реализации угроз;; - выявлять события и реагировать на инциденты информационной безопасности;; - проводить расследования по инцидентам информационной безопасности;; - оформлять необходимые документы по расследованиям инцидентов информационной безопасности..

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к основной профессиональной образовательной программе Безопасность автоматизированных 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	Введение	6	10	1	-	1	-	-	-	-	-	4	-	***Подготовка к текущему контролю:***
1.1	Введение	6		1	-	1	-	-	-	-	-	4	-	Повторение материала по разделу "Введение" ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Введение" ***Изучение материалов литературных источников:*** [2], 3-15
2	Управление инцидентами информационной безопасности	41		5	-	6	-	-	-	-	-	30	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Управление инцидентами информационной безопасности"
2.1	Инциденты информационной безопасности	6		1	-	1	-	-	-	-	-	4	-	***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка домашних заданий
2.2	Основные причины и предпосылки возникновения инцидентов информационной безопасности	4		1	-	1	-	-	-	-	-	2	-	***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
2.3	Правовые основы управления инцидентами информационной безопасности	10		1	-	1	-	-	-	-	-	8	-	

2.4	Основные способы и методы выявления инцидентов информационной безопасности	11		1	-	2	-	-	-	-	-	8	-	работам. ***Подготовка доклада, выступления:*** Задание связано с углубленным изучением разделов дисциплины и самостоятельным поиском материалов для раскрытия темы доклада. Материалы выполненной работы представляются в электронном виде или в форме распечатанных презентационных слайдов. В качестве тем докладов студентам предлагаются следующие варианты: "Средства и системы мониторинга ИБ", "Средства и системы выявления инцидентов ИБ". ***Подготовка к контрольной работе:*** Изучение материалов по разделу Управление инцидентами информационной безопасности и подготовка к контрольной работе ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Управление инцидентами информационной безопасности" ***Подготовка к практическим занятиям:*** Задания ориентированы на решения минизадач по разделу "Управление инцидентами информационной безопасности". Студенты необходимо повторить теоретический материал, разобрать примеры решения аналогичных задач. провести работы по варианту задания и сделать выводы. В качестве задания используются следующие упражнения: "Разработка плана расследования по инциденту ИБ", "Оформление акта служебного расследования по инциденту ИБ" ***Подготовка реферата:*** В рамках реферативной части студенту необходим провести обзор литературных источников по выбранной теме, комплексно осветить
2.5	Менеджмент инцидентов информационной безопасности	10		1	-	1	-	-	-	-	-	8	-	

														вопрос в соответствии с темой реферата, подготовить презентацию для выступления по результатам работы на семинарском занятии. В качестве тем реферата студенту предлагаются следующие варианты: ***Изучение материалов литературных источников:*** [2], 60-86 [3], 7-28
3	Проведение расследований инцидентов информационной безопасности	61		10	-	13	-	-	-	-	-	38	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Проведение расследований инцидентов информационной безопасности" ***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. ***Подготовка доклада, выступления:*** Задание связано с углубленным изучением разделов дисциплины и самостоятельным поиском материалов для раскрытия темы доклада. Материалы выполненной работы представляются в электронном виде или в форме распечатанных презентационных слайдов. В качестве тем докладов студентам предлагаются следующие варианты: "Проведение компьютерных экспертиз", "Порядок исследования компьютерной техники". ***Подготовка к контрольной работе:*** Изучение материалов по разделу Проведение
3.1	Правовые основы проведения расследований инцидентов информационной безопасности	4		1	-	1	-	-	-	-	-	2	-	
3.2	Реагирование на инциденты информационной безопасности	7		1	-	2	-	-	-	-	-	4	-	
3.3	Расследование инцидентов информационной безопасности.	14		2	-	4	-	-	-	-	-	8	-	
3.4	Изъятие компьютерной техники и носителей информации	14		4	-	2	-	-	-	-	-	8	-	
3.5	Проведение экспертиз при расследованиях компьютерных преступлений	11		1	-	2	-	-	-	-	-	8	-	
3.6	Основы форензики (компьютерной криминалистики)	11		1	-	2	-	-	-	-	-	8	-	

														расследований инцидентов информационной безопасности и подготовка к контрольной работе ***<u>Подготовка к практическим занятиям:</u>*** Изучение материала по разделу "Проведение расследований инцидентов информационной безопасности" подготовка к выполнению заданий на практических занятиях ***<u>Самостоятельное изучение теоретического материала:</u>*** Изучение дополнительного материала по разделу "Проведение расследований инцидентов информационной безопасности" ***<u>Изучение материалов литературных источников:</u>*** [1], 130-141 [4], 130-141
	Экзамен	36.0		-	-	-	-	2	-	-	0.5	-	33.5	
	Всего за семестр	**144.0**		**16**	**-**	**20**	**-**	**2**	**-**	**-**	**0.5**	**72**	**33.5**	
	Итого за семестр	**144.0**		**16**	**-**	**20**	**2**		**-**		**0.5**	**105.5**		

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. Введение

1.1. Введение

1.Понятие инцидента ИБ. 2.Основные стадии развития инцидентов ИБ..

2. Управление инцидентами информационной безопасности

2.1. Инциденты информационной безопасности

1.Классификация инцидентов ИБ..

2.2. Основные причины и предпосылки возникновения инцидентов информационной безопасности

1.Основные причины инцидентов ИБ. 2.Основные предпосылки возникновения инцидентов ИБ. 3.Возможные последствия инцидентов ИБ. Понятие ущерба. Виды ущерба. Оценка ущерба..

2.3. Правовые основы управления инцидентами информационной безопасности

1.Законодательство Российской Федерации в области управления инцидентами ИБ. 2.Стандарты в области управления инцидентами ИБ. 3.Рекомендации по управлению инцидентами ИБ..

2.4. Основные способы и методы выявления инцидентов информационной безопасности

1.Выявление инцидентов информационной безопасности. 2.Мониторинг информационной безопасности. 3.Организация мониторинга информационной безопасности. 4.Анализ и приоритезация инцидентов информационной безопасности..

2.5. Менеджмент инцидентов информационной безопасности

1.Понятие менеджмента инцидентов ИБ. 2.Этапы менеджмента инцидентов ИБ. 3.Использование системы менеджмента инцидентов ИБ. 4.Документация системы менеджмента инцидентов ИБ. 5.Политика менеджмента инцидентов ИБ. 6.Программа менеджмента инцидентов ИБ..

3. Проведение расследований инцидентов информационной безопасности

3.1. Правовые основы проведения расследований инцидентов информационной безопасности

1.Ответственность за нарушения в области информационных отношений. 2.Уголовный кодекс Российской Федерации. 3.Кодекс об административной ответственности Российской Федерации. 4.Гражданский кодекс Российской Федерации. 5.Трудовой кодекс Российской Федерации. 6.Порядок взаимодействия с правоохранительными органами в ходе проведения расследований инцидентов информационной безопасности. 7.Специализированные компании, проводящие расследования инцидентов информационной безопасности..

3.2. Реагирование на инциденты информационной безопасности

1.Алгоритм действий при возникновении инцидентов информационной безопасности. 2. Силы и средства реагирования на инциденты информационной безопасности.

3.3. Расследование инцидентов информационной безопасности.

1.Проведение расследований инцидентов информационной безопасности 2.Ситуации, возникающие в ходе расследования инцидента информационной безопасности. 3.Планирование расследования инцидента информационной безопасности..

3.4. Изъятие компьютерной техники и носителей информации

1.Правовые основы изъятия и исследования компьютерной техники. 2.Изъятие и исследование компьютерной техники и носителей информации. 3.Основные ошибки, встречающиеся при изъятии имущества в ходе расследования инцидента ИБ..

3.5. Проведение экспертиз при расследованиях компьютерных преступлений

1.Понятие и виды компьютерно-технических экспертиз. 2.Проведение компьютерно-технических экспертиз..

3.6. Основы форензики (компьютерной криминалистики)

1.Предмет форензики (компьютерной криминалистики). 2.Методы и средства форензики. 3.Исследование логов. 4.Обращение с короткоживущими данными..

3.3. Темы практических занятий

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

3.4. Темы лабораторных работ

не предусмотрено

3.5 Консультации

Групповые консультации по разделам дисциплины (ГК)

1. Обсуждение материалов по кейсам раздела "Введение"
2. Обсуждение материалов по кейсам раздела "Управление инцидентами информационной безопасности"
3. Обсуждение материалов по кейсам раздела "Проведение расследований инцидентов информационной безопасности"

Текущий контроль (ТК)

1. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Введение"
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:					
особенности управления инцидентами информационной безопасности применительно к различным сферам деятельности.	ПК-1.4$_{ПК-1}$			+	Контрольная работа/Контрольная работа № 2
основы управления инцидентами информационной безопасности на предприятии;	ПК-1.4$_{ПК-1}$		+		Контрольная работа/Контрольная работа № 1
требования нормативных и правовых документов (законы, стандарты, регламенты) в предметной области дисциплины;	ПК-1.4$_{ПК-1}$	+	+		Тестирование/Тест № 1
Уметь:					
оформлять необходимые документы по расследованиям инцидентов информационной безопасности.	ПК-1.4$_{ПК-1}$			+	Коллоквиум/Коллоквиум № 3
проводить расследования по инцидентам информационной безопасности;	ПК-1.4$_{ПК-1}$			+	Коллоквиум/Коллоквиум № 2
выявлять события и реагировать на инциденты информационной безопасности;	ПК-1.4$_{ПК-1}$		+		Коллоквиум/Коллоквиум № 1
определять основные виды угроз информационной безопасности, возможные методы и пути реализации угроз;	ПК-1.4$_{ПК-1}$		+		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

10 семестр

Форма реализации: Письменная работа

1. Коллоквиум № 1 (Коллоквиум)
2. Коллоквиум № 2 (Коллоквиум)
3. Коллоквиум № 3 (Коллоквиум)
4. Контрольная работа № 1 (Контрольная работа)
5. Контрольная работа № 2 (Контрольная работа)
6. Тест № 1 (Тестирование)
7. Тест № 2 (Тестирование)

Балльно-рейтинговая структура дисциплины является приложением А.

4.2 Промежуточная аттестация по дисциплине

Экзамен (Семестр №10)

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

В диплом выставляется оценка за 10 семестр.

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

5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1 Печатные и электронные издания:

1. 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 .;
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. Галатенко, В.А. Стандарты информационной безопасности. Курс лекций : учебное пособие для вузов по специальностям в области информационных технологий / В.А. Галатенко ; Ред. В. Б. Бетелин . – 2-е изд . – М. : Интернет-Ун-т информ. технологий, 2012 . – 264 с. – (Основы информационных технологий) . - ISBN 978-5-9556-0053-6 .;
4. 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. **Научная электронная библиотека** - https://elibrary.ru/
4. **База данных ВИНИТИ online** - http://www.viniti.ru/
5. **Электронные ресурсы издательства Springer** - https://link.springer.com/
6. **База данных Web of Science** - http://webofscience.com/
7. **База данных Scopus** - http://www.scopus.com
8. **ЭБС "Консультант студента"** - http://www.studentlibrary.ru/
9. **Журнал Science** - https://www.sciencemag.org/
10. **Электронная библиотека МЭИ (ЭБ МЭИ)** - http://elib.mpei.ru/login.php
11. **Портал открытых данных Российской Федерации** - https://data.gov.ru
12. **Информационно-справочная система «Кодекс/Техэксперт»** - Http:\\proinfosoft.ru; http://docs.cntd.ru/
13. **Национальный портал онлайн обучения «Открытое образование»** - https://openedu.ru
14. **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	М-510, Учебная лаборатория информационно-аналитический технологий - компьютерный класс	стул, стол письменный, мультимедийный проектор, экран, доска маркерная, компьютер персональный, кондиционер
Учебные аудитории для проведения промежуточной аттестации	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
	А-317, Учебная аудитория	парта со скамьей, 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	А-317, Учебная аудитория	парта со скамьей, стол преподавателя, стул, доска меловая
Помещения для хранения оборудования и учебного инвентаря	К-202/2, Склад кафедры БИТ	стеллаж для хранения инвентаря, стол, стул, шкаф для документов, шкаф для хранения инвентаря, тумба, запасные комплектующие для оборудования

Приложение А

БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА ДИСЦИПЛИНЫ

Управление инцидентами информационной безопасности

(название дисциплины)

10 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:

КМ-1 Контрольная работа № 1 (Контрольная работа)
КМ-1 Тест № 1 (Тестирование)
КМ-2 Контрольная работа № 2 (Контрольная работа)
КМ-2 Тест № 2 (Тестирование)
КМ-3 Коллоквиум № 1 (Коллоквиум)
КМ-4 Коллоквиум № 3 (Коллоквиум)
КМ-4 Коллоквиум № 2 (Коллоквиум)

Вид промежуточной аттестации – Экзамен.

Номер раздела	Раздел дисциплины	Индекс КМ:	КМ-1	КМ-1	КМ-2	КМ-2	КМ-3	КМ-4	КМ-4
		Неделя КМ:	4	4	8	8	12	15	15
1	Введение								
1.1	Введение			+					
2	Управление инцидентами информационной безопасности								
2.1	Инциденты информационной безопасности		+	+		+	+		
2.2	Основные причины и предпосылки возникновения инцидентов информационной безопасности		+	+		+	+		
2.3	Правовые основы управления инцидентами информационной безопасности		+	+		+	+		
2.4	Основные способы и методы выявления инцидентов информационной безопасности		+	+		+	+		
2.5	Менеджмент инцидентов информационной безопасности		+	+		+	+		
3	Проведение расследований инцидентов информационной безопасности								
3.1	Правовые основы проведения расследований инцидентов информационной безопасности				+			+	+
3.2	Реагирование на инциденты информационной безопасности				+			+	+

3.3	Расследование инцидентов информационной безопасности.			+			+	+
3.4	Изъятие компьютерной техники и носителей информации			+			+	+
3.5	Проведение экспертиз при расследованиях компьютерных преступлений			+			+	+
3.6	Основы форензики (компьютерной криминалистики)			+			+	+
	Вес КМ, %:	15	10	15	10	25	15	10