Министерство науки и высшего образования РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Национальный исследовательский университет «МЭИ»

Направление подготовки/специальность: 01.04.02 Прикладная математика и информатика

Наименование образовательной программы: Искусственный интеллект

Уровень образования: высшее образование - магистратура

Форма обучения: Очная

Рабочая программа дисциплины
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СИСТЕМ

Блок:	**Блок 1 «Дисциплины (модули)»**
Часть образовательной программы:	**Часть, формируемая участниками образовательных отношений**
№ дисциплины по учебному плану:	**Б1.Ч.01**
Трудоемкость в зачетных единицах:	**1 семестр - 3;**
Часов (всего) по учебному плану:	**108 часов**
Лекции	**1 семестр - 16 часов;**
Практические занятия	**не предусмотрено учебным планом**
Лабораторные работы	**1 семестр - 32 часа;**
Консультации	**проводится в рамках часов аудиторных занятий**
Самостоятельная работа	**1 семестр - 59,7 часа;**
в том числе на КП/КР	**не предусмотрено учебным планом**
Иная контактная работа	**проводится в рамках часов аудиторных занятий**
включая: **Лабораторная работа**	
Промежуточная аттестация:	
Зачет с оценкой	**1 семестр - 0,3 часа;**

Москва 2024

ПРОГРАММУ СОСТАВИЛ:

Преподаватель	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Сергеев А.В. Идентификатор: R45d170df-SergeevAVad-0ce1748	А.В. Сергеев

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Варшавский П.Р. Идентификатор: R9a563c96-VarshavskyPR-efb4bbd	П.Р. Варшавский
Заведующий выпускающей кафедрой	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Варшавский П.Р. Идентификатор: R9a563c96-VarshavskyPR-efb4bbd	П.Р. Варшавский

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель освоения дисциплины: изучение современных методов и средств защиты информации, включая криптографию, стеганографию, управление доступом, а также формирование навыков реагирования на инциденты информационной безопасности.

Задачи дисциплины

- Освоение методологии разработки модели угроз и модели нарушителя информационной безопасности;
- Получение навыков оценки защищенности продуктов информационных технологий и проектных решений по обеспечению информационной безопасности;
- Развитие компетенций в сфере использования передовых инструментов и техник защиты информации, включая обнаружение и предотвращение несанкционированного доступа.

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 Способен выполнять работы на всем жизненном цикле информационных систем в выбранной среде разработки компьютерного ПО	ИД-2$_{ПК-1}$ Демонстрирует знание современных программно-технических средств, информационных технологий и тенденции их развития	знать: - Методы обнаружения угроз информационной системы; - Базовые структуры данных и механизмы поиска информации. уметь: - Проводить исследования компьютерных систем; - Использовать результаты журналов событий операционной системы в рамках оценки информационной безопасности компьютерных систем.
ПК-1 Способен выполнять работы на всем жизненном цикле информационных систем в выбранной среде разработки компьютерного ПО	ИД-3$_{ПК-1}$ Демонстрирует умение выбирать и обосновывать выбор программно-технической среды реализации проектов по информационным технологиям	знать: - Методы и средства стеганографии; - Методы и средства защиты информационных процессов в компьютерных системах. уметь: - Применять средства защиты информации; - Комбинировать и адаптировать современные информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к основной профессиональной образовательной программе Искусственный интеллект (далее – ОПОП), направления подготовки 01.04.02 Прикладная математика и информатика, уровень образования: высшее образование - магистратура.

Требования к входным знаниям и умениям:

- знать Основные понятия и положения теории информации и теории кодирования для анализа методов и способов кодирования и декодирования
- знать Принципы построения и состав операционных систем
- знать Структура и типы файловых систем
- знать Способы несанкционированного доступа к данным и способы идентификации и аутентификации пользователей компьютерных систем и сетей
- уметь Использовать средства операционных систем при решении различных прикладных задач
- уметь Использовать литературу и источники сети Интернет для получения информации о создании новых методов и средств защиты информации
- уметь Использовать методы и средства криптографической защиты информации
- уметь Использовать средства анализа защищенности компьютерных систем и сетей

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 3 зачетных единицы, 108 часов.

№ 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	Основные методы реализации защиты информации в компьютерных системах.	32	1	4	8	-	-	-	-	-	-	20	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Основные методы реализации защиты информации в компьютерных системах." Подготовка отчета о выполнении лабораторной работы №1 ***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Основные методы реализации защиты информации в компьютерных системах." ***Изучение материалов литературных источников:*** [1], 196-204 [6], 4-6 [7], 22-29 [11], 32-54 [12], 38-56 [15], 12-27
1.1	Основные методы реализации защиты информации в компьютерных системах.	32		4	8	-	-	-	-	-	-	20	-	
2	Криптографические методы защиты информации.	27		4	8	-	-	-	-	-	-	15	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Криптографические методы защиты информации." Изучение правктического материала по анализу данных в структурах данных и криптоанализу
2.1	Криптографические методы защиты информации.	27		4	8	-	-	-	-	-	-	15	-	

														Подготовка к лабораторной работе: Для выполнения заданий по лабораторной работе необходимо предварительно изучить темы лекций и набор инструментов для анализа поставленной задачи по лабораторной работы №2, а так же изучить методы и подходы к рещению задач в научной литературе ***Изучение материалов литературных источников:*** [4], 20-26 [5], 142-151 [10], 43-62 [11], 63-78
3	Методы скрытия информации в цифровых носителях и их анализ.	22		4	8	-	-	-	-	-	-	10	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Методы скрытия информации в цифровых носителях и их анализ." Подготовка ответов на контрольные вопросы к защите лабораторной работы №3. ***Подготовка к лабораторной работе:*** Для выполнения заданий по лабораторной работе необходимо предварительно изучить задачи и вопросы по лабораторной работы №3 и подготовить необходимый набор программных средств ***Изучение материалов литературных источников:*** [2], 56-67 [3], 20-39 [6], 188-204 [8], 10-22 [11], 152-160
3.1	Методы скрытия информации в цифровых носителях и их анализ	22		4	8	-	-	-	-	-	-	10	-	
4	Методы расследования инцидентов информационной безопасности.	26.7		4	8	-	-	-	-	-	-	14.7	-	***Подготовка к текущему контролю:*** Подготовка отчета о выполнении лаболаторной работы №4. ***Подготовка к лабораторной работе:*** Для выполнения заданий по лабораторной работе необходимо предварительно изучить тему и
4.1	Методы	26.7		4	8	-	-	-	-	-	-	14.7	-	

	расследования инцидентов информационной безопасности.													задачи выполнения лабораторной работы, а так же изучить вопросы вариантов обработки результатов по изученному в разделе "Методы расследования инцидентов информационной безопасности." материалу. ***<u>Самостоятельное изучение теоретического материала:</u>*** Изучение дополнительного материала по разделу "Методы расследования инцидентов информационной безопасности.", а также материала исследований и работ в соответствии с поставленными задачами Лаболаторной работы №4. ***<u>Изучение материалов литературных источников:</u>*** [7], 230-241 [9], 8-16 [13], 42-61 [14], 80-93
	Зачет с оценкой	0.3		-	-	-	-	-	-	-	0.3	-	-	
	Всего за семестр	**108.0**		**16**	**32**	**-**	**-**	**-**	**-**	**-**	**0.3**	**59.7**	**-**	
	Итого за семестр	**108.0**		**16**	**32**	**-**	**-**		**-**		**0.3**	**59.7**		

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. Основные методы реализации защиты информации в компьютерных системах.

1.1. Основные методы реализации защиты информации в компьютерных системах.

Угрозы информационной безопасности, каналы утечки информации и факторы, воздействующие на информацию. Классификация методов и средств защиты информации.. Организационные меры защиты информации. Менеджмент событий и инцидентов информационной безопасности. Специфика программных средств. Журналы событий как источник информации.. Групповая политика безопасности. Методы анализа данных безопасности. Выявление угроз и уязвимостей..

2. Криптографические методы защиты информации.

2.1. Криптографические методы защиты информации.

Криптографические методы защиты информации. Применение и обзор современных симметричных криптосистем. Генераторы псевдослучайных чисел их применение в криптографии. Обзор и возможности средств криптографической защиты информации.. Основы структуры данных различных файловых форматов и их безопасность..

3. Методы скрытия информации в цифровых носителях и их анализ.

3.1. Методы скрытия информации в цифровых носителях и их анализ

Основы стеганографии и скрытых каналов. Основные методы скрытия информации. Обзор стеганографических методов и алгоритов. Применение стеганографии в реальном мире. Файловые системы, классификация. Виды и особенности файловых систем..

4. Методы расследования инцидентов информационной безопасности.

4.1. Методы расследования инцидентов информационной безопасности.

Концепция и базовые подходы в расследование инцидентов информационной безопасности. Методология расследования инцидентов. Инструменты и технологии расследования. Основные подходы к анализу метаданных и структуры файлов..

3.3. Темы практических занятий

не предусмотрено

3.4. Темы лабораторных работ

1. Оценка безопасности информационной системы;
2. Криптографические средства защиты информации и анализ защиты данных;
3. Стеганография. Программные средства и методы;
4. Компьютерная криминалистика.

3.5 Консультации

Групповые консультации по разделам дисциплины (ГК)

1. Обсуждение материалов по кейсам раздела "Основные методы реализации защиты информации в компьютерных системах."
2. Обсуждение материалов по кейсам раздела "Криптографические методы защиты информации."

3. Обсуждение материалов по кейсам раздела "Методы скрытия информации в цифровых носителях и их анализ."

Текущий контроль (ТК)

1. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Основные методы реализации защиты информации в компьютерных системах."
2. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Криптографические методы защиты информации."
3. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Методы скрытия информации в цифровых носителях и их анализ."
4. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Методы расследования 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	4	
Знать:						
Базовые структуры данных и механизмы поиска информации	ИД-2$_{ПК-1}$		+			Лабораторная работа/Криптографические средства защиты информации и анализ защиты данных
Методы обнаружения угроз информационной системы	ИД-2$_{ПК-1}$	+				Лабораторная работа/Оценка безопасности информационной системы
Методы и средства защиты информационных процессов в компьютерных системах	ИД-3$_{ПК-1}$		+			Лабораторная работа/Криптографические средства защиты информации и анализ защиты данных
Методы и средства стеганографии	ИД-3$_{ПК-1}$			+		Лабораторная работа/Стеганография. Программные средства и методы
Уметь:						
Использовать результаты журналов событий операционной системы в рамках оценки информационной безопасности компьютерных систем	ИД-2$_{ПК-1}$				+	Лабораторная работа/Компьютерная криминалистика
Проводить исследования компьютерных систем	ИД-2$_{ПК-1}$	+				Лабораторная работа/Оценка безопасности информационной системы
Комбинировать и адаптировать современные информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности	ИД-3$_{ПК-1}$				+	Лабораторная работа/Компьютерная криминалистика
Применять средства защиты информации	ИД-3$_{ПК-1}$			+		Лабораторная работа/Стеганография. Программные средства и методы

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

4.1. Текущий контроль успеваемости

1 семестр

Форма реализации: Компьютерное задание

1. Компьютерная криминалистика (Лабораторная работа)
2. Криптографические средства защиты информации и анализ защиты данных (Лабораторная работа)
3. Оценка безопасности информационной системы (Лабораторная работа)
4. Стеганография. Программные средства и методы (Лабораторная работа)

Балльно-рейтинговая структура дисциплины является приложением А.

4.2 Промежуточная аттестация по дисциплине

Зачет с оценкой (Семестр №1)

Определяется по совокупности результатов текущего контроля успеваемости в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ»

В диплом выставляется оценка за 1 семестр.

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

5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1 Печатные и электронные издания:

1. Бабаш, А. В. Информационная безопасность : история специальных методов криптографической деятельности : учебное пособие / А. В. Бабаш, Е. К. Баранова, Д. А. Ларин . – Москва : РИОР : ИНФРА-М, 2024 . – 236 с. – (Высшее образование) . - ISBN 978-5-369-01788-3 .;
2. В. Г. Грибунин, И. Н. Оков, И. В. Туринцев- "Цифровая стеганография", Издательство: "СОЛОН-ПРЕСС", Москва, 2009 - (264 с.)
https://biblioclub.ru/index.php?page=book&id=117549;
3. Сергеев, А. В. Криптографические и стеганографические средства защиты данных : учебное пособие по курсу "Защита данных" по направлению 01.03.02 "Прикладная математика и информатика" / А. В. Сергеев, П. Б. Хорев, Нац. исслед. ун-т "МЭИ" (НИУ"МЭИ") . – Москва : Изд-во МЭИ, 2023 . – 72 с. - ISBN 978-5-7046-2819-4 .
http://elib.mpei.ru/elib/view.php?id=12475;
4. Хорев, П. Б. Криптографические методы защиты информации : практикум по курсу "Криптографические методы защиты информации" по направлению 01.03.02 "Прикладная математика и информатика" / П. Б. Хорев, Нац. исслед. ун-т "МЭИ" (НИУ"МЭИ") . – Москва : Изд-во МЭИ, 2020 . – 52 с. - ISBN 978-5-7046-2321-2 .
http://elib.mpei.ru/elib/view.php?id=11319;
5. Фомичев, В. М. Криптографические методы защиты информации: [в 2-х ч.] : учебник для студентов вузов, обучающихся по инженерно-техническим направлениям / В. М. Фомичев, Д. А. Мельников ; ред. В. М. Фомичев . – Москва : Юрайт, 2024 . – (Высшее образование) . - ISBN 978-5-9916-7089-0 . Ч. 1 : Математические аспекты / В. М. Фомичев, Д. А. Мельников . – 2024 . – 209 с. - ISBN 978-5-9916-7088-3 .;

6. Стеганография, цифровые водяные знаки и стеганоанализ / А. В. Аграновский, [и др.] . – М. : Вузовская книга, 2009 . – 220 с. - ISBN 978-5-9502-0401-2 .;
7. Мельников, Д. А. Информационные процессы в компьютерных сетях : Протоколы,стандарты, интерфейсы, модели... / Д. А. Мельников . – М. : Кудиц-Образ, 1999 . – 256 с. – (Б-ка профессионала) . - ISBN 5-933780-02-2 : 68.90 .;
8. Грибунин, В. Г. Цифровая стеганография / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев . – М. : Солон-Пресс, 2002 . – 272 с. – (Аспекты защиты) . - ISBN 5-9800301-1-5 .;
9. Хорев, П. Б. Объектно-ориентированное программирование : учебное пособие по направлению "Информатика и вычислительная техника" / П. Б. Хорев . – 4-е изд., стер . – М. : Академия, 2012 . – 448 с. – (Высшее профессиональное образование . Бакалавриат) . - ISBN 978-5-7695-9265-2 .;
10. Шнайер, Б. Прикладная криптография : протоколы, алгоритмы и исходные коды на языке С : пер. с англ. / Б. Шнайер . – 2-е изд . – Москва; Санкт-Петербург : Диалектика, 2022 . – 1040 с. - Юбилейный выпуск к 20-летию книги . – Параллельн. тит. л. англ. - ISBN 978-5-9908462-4-1 .;
11. Рябко Б. Я., Фионов А. Н.- "Основы современной криптографии и стеганографии", (2-е изд.), Издательство: "Горячая линия-Телеком", Москва, 2016 - (232 с.) https://e.lanbook.com/book/111098;
12. Бахаров Л. Е.- "Информационная безопасность и защита информации (разделы криптография и стеганография)", Издательство: "МИСИС", Москва, 2019 - (59 с.) https://e.lanbook.com/book/116907;
13. "Компьютерная криминалистика", Издательство: "СКФУ", Ставрополь, 2017 - (84 с.) https://e.lanbook.com/book/155227;
14. Иванюгин В. М.- "Администрирование безопасности ОС Windows инструментальными средствами", Издательство: "РТУ МИРЭА", Москва, 2020 - (104 с.) https://e.lanbook.com/book/163832;
15. "Стеганографические и криптографические методы защиты информации", Издательство: "БГПУ имени М. Акмуллы", Уфа, 2016 - (112 с.) https://e.lanbook.com/book/90963.

5.2 Лицензионное и свободно распространяемое программное обеспечение:
1. Acrobat Reader;
2. Kali Linux;
3. Libre Office;
4. FAR Manager;
5. 7-zip.

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. **Электронные ресурсы издательства Springer** - https://link.springer.com/
5. **База данных Web of Science** - http://webofscience.com/
6. **База данных Scopus** - http://www.scopus.com
7. **База данных IEL издательства IEEE (Institute of Electrical and Electronics Engineers, Inc.)** - https://ieeexplore.ieee.org/Xplore/home.jsp?reload=true
8. **Электронная библиотека МЭИ (ЭБ МЭИ)** - http://elib.mpei.ru/login.php

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Тип помещения	Номер аудитории, наименование	Оснащение
Учебные аудитории для проведения лекционных занятий и текущего контроля	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
	Г-403, Учебная аудитория	парта со скамьей, стол преподавателя, стул, доска меловая, компьютерная сеть с выходом в Интернет
Учебные аудитории для проведения лабораторных занятий	М-708, Дисплейный класс каф. "ПМИИ"	стол преподавателя, стол компьютерный, стул, компьютерная сеть с выходом в Интернет, мультимедийный проектор, экран, компьютер персональный, кондиционер
	М-706, Дисплейный класс каф. "ПМИИ"	стол преподавателя, стол компьютерный, стул, компьютерная сеть с выходом в Интернет, мультимедийный проектор, экран, компьютер персональный, кондиционер
Учебные аудитории для проведения промежуточной аттестации	М-706, Дисплейный класс каф. "ПМИИ"	стол преподавателя, стол компьютерный, стул, компьютерная сеть с выходом в Интернет, мультимедийный проектор, экран, компьютер персональный, кондиционер
Помещения для самостоятельной работы	НТБ-201, Компьютерный читальный зал	стол компьютерный, стул, стол письменный, вешалка для одежды, компьютерная сеть с выходом в Интернет, компьютер персональный, принтер, кондиционер
Помещения для консультирования	М-704, Преподавательская кафедры ПМИИ	стол, стул, шкаф, тумба, доска меловая, компьютерная сеть с выходом в Интернет, мультимедийный проектор, экран, компьютер персональный, холодильник, кондиционер
Помещения для хранения оборудования и учебного инвентаря	М-703а/1, Кладовая каф. "ПМИИ"	стеллаж для хранения книг, тумба, экран, ноутбук, книги, учебники, пособия

Приложение А

БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА ДИСЦИПЛИНЫ

Информационная безопасность компьютерных систем

(название дисциплины)

1 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:

КМ-1 Оценка безопасности информационной системы (Лабораторная работа)
КМ-2 Криптографические средства защиты информации и анализ защиты данных (Лабораторная работа)
КМ-3 Стеганография. Программные средства и методы (Лабораторная работа)
КМ-4 Компьютерная криминалистика (Лабораторная работа)

Вид промежуточной аттестации – Зачет с оценкой.

Номер раздела	Раздел дисциплины	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
		Неделя КМ:	4	8	12	16
1	Основные методы реализации защиты информации в компьютерных системах.					
1.1	Основные методы реализации защиты информации в компьютерных системах.		+			
2	Криптографические методы защиты информации.					
2.1	Криптографические методы защиты информации.			+		
3	Методы скрытия информации в цифровых носителях и их анализ.					
3.1	Методы скрытия информации в цифровых носителях и их анализ				+	
4	Методы расследования инцидентов информационной безопасности.					
4.1	Методы расследования инцидентов информационной безопасности.					+
		Вес КМ, %:	30	20	20	30