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

Направление подготовки/специальность: 09.03.01 Информатика и вычислительная техника

Наименование образовательной программы: Вычислительные машины, комплексы, системы и сети

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очная

Рабочая программа дисциплины
МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Блок:	**Блок 1 «Дисциплины (модули)»**
Часть образовательной программы:	**Часть, формируемая участниками образовательных отношений**
№ дисциплины по учебному плану:	**Б1.Ч.08**
Трудоемкость в зачетных единицах:	**7 семестр - 4;**
Часов (всего) по учебному плану:	**144 часа**
Лекции	**7 семестр - 16 часов;**
Практические занятия	**не предусмотрено учебным планом**
Лабораторные работы	**7 семестр - 16 часов;**
Консультации	**проводится в рамках часов аудиторных занятий**
Самостоятельная работа	**7 семестр - 111,7 часов;**
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	**7 семестр - 0,3 часа;**

Москва 2025

ПРОГРАММУ СОСТАВИЛ:

Преподаватель	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Пайков А.С. Идентификатор: R02d5e50d-PaikovAS-2468ee70	А.С. Пайков

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Гольцов А.Г. Идентификатор: R64210572-GoltsovAG-cebbd3e8	А.Г. Гольцов
Заведующий выпускающей кафедрой	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Вишняков С.В. Идентификатор: R35b26072-VishniakovSV-02810d9	С.В. Вишняков

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель освоения дисциплины: Изучение математических основ криптологии, изучение основ информационной безопасности компьютерных систем, формирование у слушателей знаний и навыков, которые необходимы для эффективного применения средств защиты информации от несанкционированного доступа..

Задачи дисциплины

- изучение алгебраических и информационных основ криптологии, а также элементов теории вероятности и теории сложности;
- освоение классификации защищаемой информации, её свойств и правовых вопросов, связанных с защитой информации;
- изучение основных принципов обеспечения безопасности автоматизированных систем обработки информации;
- реализация парольных систем в целях защиты информации от 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 обосновывать принимаемые проектные решения, осуществлять постановку и выполнять эксперименты по проверке их корректности и эффективности	ИД-З$_{ПК-1}$ Производит оценку влияния применяемых технических решений на общее функционирование системы	знать: - способы и технологии применения криптографии в решении задач идентификации и аутентификации, частотные характеристики языков и их использование при построении систем парольной защиты. уметь: - использовать современные информационные технологии при решении задач защиты информации; формализовать задачу по защите информации; применять стандарты по оценке защищенности АСОИ при анализе и проектировании систем защиты информации в АСОИ.
ПК-2 Способен решать вопросы управления безопасностью сетевых устройств и программного обеспечения при их проектировании	ИД-1$_{ПК-2}$ Демонстрирует знание нормативной базы, методов описания, анализа и проектирования в области обеспечения безопасности информационных систем и компьютерной криптографии	знать: - методологические и технологические основы обеспечения безопасности АСОИ; угрозы и методы нарушения безопасности АСОИ; стандарты по оценке защищенных систем. уметь: - обосновывать принимаемые проектные решения; применять математический аппарат, в том числе с использованием вычислительной техники, для решения профессиональных задач, разрабатывать модели открытого текста различного

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Запланированные результаты обучения
		уровня сложности; проводить обработку открытого текста для подготовки к операциям шифрования.
ПК-2 Способен решать вопросы управления безопасностью сетевых устройств и программного обеспечения при их проектировании	ИД-2$_{ПК-2}$ Демонстрирует знание методов и средств обеспечения защиты носителей информации, ЭВМ и компьютерных сетей от несанкционированного доступа	знать: - показатели эффективности принимаемого проектного решения; понятия группы, кольца, поля ; качественные и количественные свойства информации; статистические модели открытого текста. уметь: - – инсталлировать, тестировать, испытывать и использовать программно-аппаратные средства вычислительных и информационных систем и подсистем их защиты.
ПК-2 Способен решать вопросы управления безопасностью сетевых устройств и программного обеспечения при их проектировании	ИД-4$_{ПК-2}$ Осуществляет разработку аппаратных и программных средств, необходимых для обеспечения безопасности компьютерных систем	знать: - угрозы и методы нарушения безопасности АИС; методы и средства обеспечения защиты носителей информации; методы и алгоритмы уничтожения конфиденциальной информации. уметь: - использовать современные инструментальные средства и технологии программирования.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к основной профессиональной образовательной программе Вычислительные машины, комплексы, системы и сети (далее – ОПОП), направления подготовки 09.03.01 Информатика и вычислительная техника, уровень образования: высшее образование - бакалавриат.

Требования к входным знаниям и умениям:
- знать Дискретную математику
- знать Информатику
- знать Схемотехнику
- знать Программирование
- уметь конвертировать данные из одной системы счисления в другую
- уметь вводить и обрабатывать информацию средствами операционной системы
- уметь разрабатывать алгоритмы обработки данных сложной структуры
- уметь работать с виртуальными средами

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	Основы информационной безопасности: нормативные и технические аспекты	35	7	4	4	-	-	-	-	-	-	27	-	***Подготовка к аудиторным занятиям:*** Подготовка к защите лаб. раб. № 9,10, [8], стр. 12-20, [2] стр 181-188 ***Подготовка к контрольной работе:*** Подготовка к защите лаб. раб. № 6, 7, КЗ32
1.1	Основы информационной безопасности: нормативные и технические аспекты	35		4	4	-	-	-	-	-	-	27	-	***Подготовка к аудиторным занятиям:*** Подготовка к защите лаб. раб. № 5 [1], стр. 63-96 ***Подготовка к аудиторным занятиям:*** Подготовка к защите лабораторных работ № 1,2,3 КЗ31 [1], стр. 12-62; ***Изучение материалов литературных источников:*** [1], 5 [7], 20 [8], 1-140
2	Криптография и защита данных	35.7		4	4	-	-	-	-	-	-	27.7	-	***Подготовка к аудиторным занятиям:*** Подготовка к защите лаб. раб. № 11,12,13 [8], стр. 111-158, ***Изучение материалов литературных источников:*** [5], 15-19 [6], 256-312
2.1	Криптография и защита данных	35.7		4	4	-	-	-	-	-	-	27.7	-	
3	Практические аспекты и современные угрозы	36		4	4	-	-	-	-	-	-	28	-	***Подготовка к аудиторным занятиям:*** Подготовка к защите лаб. раб. № 9,10, [8], стр. 12-20, [2] стр 181-188 ***Изучение материалов литературных источников:***
3.1	Практические аспекты и современные угрозы	36		4	4	-	-	-	-	-	-	28	-	

														[3], 156-214 [4], 1-16
4	Аудит и управление информационной безопасностью	37		4	4	-	-	-	-	-	-	29	-	***Изучение материалов литературных источников:*** [2], 200-345
4.1	Аудит и управление информационной безопасностью	37		4	4	-	-	-	-	-	-	29	-	
	Зачет с оценкой	0.3		-	-	-	-	-	-	-	0.3	-	-	
	Всего за семестр	**144.0**		**16**	**16**	-	-	-	-	-	**0.3**	**111.7**	-	
	Итого за семестр	**144.0**		**16**	**16**	-	-		-		**0.3**	**111.7**		

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. Основы информационной безопасности: нормативные и технические аспекты

1.1. Основы информационной безопасности: нормативные и технические аспекты

Множества и отображения. Сюръекция, инъекция, биекция. Бинарные отношения. Бинарные операции. Алгебраические структуры. Полугруппы и моноиды. Группа, абелева группа, циклическая и конечная группа. Кольца, идеал. Поля, примеры полей, образующий элемент, простые поля. Парадокс дней рождений. Лямбда – алгоритм Полларда. Функция возведения в степень по модулю. Математические модели открытого текста. Частотные характеристики. Вероятностная модель первого приближения. Теория сложности. Большие числа. Сложность алгоритмов. Сложность проблем. Машина Тьюринга. Детерминированное полиномиальное время. Полиномиальные вычислительные задачи. Оценки сложности основных операций в модулярной арифметике. Недетерминированное полиномиальное время. Классы сложности..

2. Криптография и защита данных

2.1. Криптография и защита данных

Типы секретных систем. Обзор литературы. Определение информации. Классификация защищаемой информации и ее носителей. Правовая основа. Государственная тайна. Коммерческая тайна. Информация как продукт. Характеристики информации. Количество информации в сообщении. Энтропия и неопределенность. Избыточность информации. Энтропия языка. Стойкость криптосистем. Расстояние единственности. Основные понятия. Политика безопасности. Основные угрозы безопасности АСОИ. Компоненты АСОИ. Основные каналы несанкционированного доступа. Обеспечение безопасности АСОИ. Матрица доступа. Домен безопасности. Основы проектирования системы защиты АСОИ. Меры обеспечения безопасности компьютерных систем. Классы защищенности АСОИ. Подсистема управления доступом. Подсистема регистрации и учета. Подсистема криптографической защиты. Подсистема обеспечения целостности. Хранение секретов. Безопасность хранения информации на жестких дисках. Методы уничтожения информации на НЖМД. Алгоритм Гутманна..

3. Практические аспекты и современные угрозы

3.1. Практические аспекты и современные угрозы

Парольные системы для защиты от несанкционированного доступа к информации. Основные термины. Методы аутентификации. Биометрические методы. Требования к выбору и использованию паролей. Длина паролей и безопасное время. Хранение паролей. Хэш-функция. Аутентификация "с нулевым разглашением". Противодействие пассивному перехвату. Защита при компрометации проверяющего. Противодействие несанкционированному воспроизведению. Одноразовые пароли. Метод «запрос-ответ»..

4. Аудит и управление информационной безопасностью

4.1. Аудит и управление информационной безопасностью

Аудит и управление информационной безопасностью.

3.3. Темы практических занятий

не предусмотрено

3.4. Темы лабораторных работ

1. Лабораторная работа МСЗИ №1 “Криптографические шифры”;
2. Лабораторная работа МСЗИ №2 “SNS. Базовый функционал”;
3. Лабораторная работа МСЗИ №3 “SNS. Продвинутые функции”;
4. Лабораторная работа МСЗИ №4 “Сетевые средства защиты”.

3.5 Консультации

Групповые консультации по разделам дисциплины (ГК)

1. Обсуждение материалов по кейсам раздела "Математические основы криптологии"
2. Обсуждение материалов по кейсам раздела "Информационная безопасность компьютерных систем"
3. Обсуждение материалов по кейсам раздела "Парольные системы"

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:						
способы и технологии применения криптографии в решении задач идентификации и аутентификации, частотные характеристики языков и их использование при построении систем парольной защиты	ИД-3$_{ПК-1}$	+				Лабораторная работа/Контроль посещения лекций №1-2 по курсу МСЗИ; Контроль выполнения лабораторной работы №1 по курсу МСЗИ (25%)
методологические и технологические основы обеспечения безопасности АСОИ; угрозы и методы нарушения безопасности АСОИ; стандарты по оценке защищенных систем	ИД-1$_{ПК-2}$	+				Лабораторная работа/Контроль посещения лекций №1-2 по курсу МСЗИ; Контроль выполнения лабораторной работы №1 по курсу МСЗИ (25%)
показатели эффективности принимаемого проектного решения; понятия группы, кольца, поля ; качественные и количественные свойства информации; статистические модели открытого текста	ИД-2$_{ПК-2}$	+				Лабораторная работа/Контроль посещения лекций №1-2 по курсу МСЗИ; Контроль выполнения лабораторной работы №1 по курсу МСЗИ (25%)
угрозы и методы нарушения безопасности АИС; методы и средства обеспечения защиты носителей информации; методы и алгоритмы уничтожения конфиденциальной информации	ИД-4$_{ПК-2}$		+			Лабораторная работа/Контроль посещения лекций №3-4 по курсу МСЗИ; Контроль выполнения лабораторной работы №2 по курсу МСЗИ (25%)
Уметь:						
использовать современные информационные технологии при решении задач защиты информации; формализовать задачу по защите информации; применять стандарты по оценке защищенности АСОИ при анализе и проектировании систем	ИД-3$_{ПК-1}$		+			Лабораторная работа/Контроль посещения лекций №3-4 по курсу МСЗИ; Контроль выполнения лабораторной работы №2 по курсу

защиты информации в АСОИ						МСЗИ (25%)
обосновывать принимаемые проектные решения; применять математический аппарат, в том числе с использованием вычислительной техники, для решения профессиональных задач, разрабатывать модели открытого текста различного уровня сложности; проводить обработку открытого текста для подготовки к операциям шифрования	ИД-1$_{ПК-2}$		+			Лабораторная работа/Контроль посещения лекций №3-4 по курсу МСЗИ; Контроль выполнения лабораторной работы №2 по курсу МСЗИ (25%)
– инсталлировать, тестировать, испытывать и использовать программно-аппаратные средства вычислительных и информационных систем и подсистем их защиты	ИД-2$_{ПК-2}$			+		Лабораторная работа/Контроль посещения лекций №5-6 по курсу МСЗИ; Контроль выполнения лабораторной работы №3 по курсу МСЗИ (25%)
использовать современные инструментальные средства и технологии программирования	ИД-4$_{ПК-2}$				+	Лабораторная работа/Контроль посещения лекций №7-8 по курсу МСЗИ; Контроль выполнения лабораторной работы №4 по курсу МСЗИ (25%)

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

4.1. Текущий контроль успеваемости

7 семестр

Форма реализации: Соблюдение графика выполнения задания

1. Контроль посещения лекций №1-2 по курсу МСЗИ; Контроль выполнения лабораторной работы №1 по курсу МСЗИ (25%) (Лабораторная работа)
2. Контроль посещения лекций №3-4 по курсу МСЗИ; Контроль выполнения лабораторной работы №2 по курсу МСЗИ (25%) (Лабораторная работа)
3. Контроль посещения лекций №5-6 по курсу МСЗИ; Контроль выполнения лабораторной работы №3 по курсу МСЗИ (25%) (Лабораторная работа)
4. Контроль посещения лекций №7-8 по курсу МСЗИ; Контроль выполнения лабораторной работы №4 по курсу МСЗИ (25%) (Лабораторная работа)

Балльно-рейтинговая структура дисциплины является приложением А.

4.2 Промежуточная аттестация по дисциплине

Зачет с оценкой (Семестр №7)

Итоговая оценка по курсу может быть рассчитана как среднее от текущей успеваемости и итогов промежуточной аттестации по 100 балльной шкале. Текущая успеваемость также рассчитывается как среднее по трем модулям по 100 бальной шкале. Только после этого можно переходить к 5-и балльной шкале. Промежуточное округление оценок в 5-и балльной системе и нелинейная шкала оценок в БАРС приводят к существенному завышению результирующих оценок.

В диплом выставляется оценка за 7 семестр.

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

5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1 Печатные и электронные издания:

1. Бондаренко И. С., Демчишин Ю. В.- "Методы и средства защиты информации", Издательство: "МИСИС", Москва, 2018 - (32 с.)
https://e.lanbook.com/book/115269;
2. Лось, А. Б. Криптографические методы защиты информации : учебник для академического бакалавриата вузов по инженерно-техническим направлениям и специальностям / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков, Нац. исслед. ун-т "Высшая школа экономики". – 2-е изд., испр. – М. : Юрайт, 2018. – 473 с. – (Бакалавр. Академический курс). – ISBN 978-5-534-01530-0.;
3. Хорев, П. Б. Методы и средства защиты информации в компьютерных системах : учебное пособие для вузов по направлению 230100(654600) "Информатика и вычислительная техника" / П. Б. Хорев. – 4-е изд., стер. – М. : АКАДЕМИЯ, 2008. – 256 с. – (Высшее профессиональное образование). – ISBN 978-5-7695-5118-5.;
4. Рытов, А. А. Парадокс дней рождений. Лабораторная работа №4 : методическое пособие по курсу "Методы и средства защиты информации" по направлению "Информатика и

вычислительная техника" / А. А. Рытов, И. А. Яшин, Нац. исслед. ун-т "МЭИ". – М. : Изд-во МЭИ, 2014. – 16 с.;
5. Романец, Ю. В. Защита информации в компьютерных системах и сетях / Ю. В. Романец, П. А. Тимофеев, В. Ф. Шаньгин. – М. : Радио и связь, 1999. – 328 с. – ISBN 5-256-01436-6 : 53.00.;
6. Шнайер, Б. Прикладная криптография: Протоколы, алгоритмы, исходные тексты на языке Си : пер. с англ. / Б. Шнайер. – М. : Триумф, 2002. – 816 с. – ISBN 5-89392-055-4.;
7. Костин В. Н.- "Методы и средства защиты компьютерной информации: информационная безопасность компьютерных сетей", Издательство: "МИСИС", Москва, 2018 - (31 с.) https://e.lanbook.com/book/116743;
8. А. Б. Арзуманян- "Международные стандарты правовой защиты информации и информационных технологий", Издательство: "Южный федеральный университет", Ростов-на-Дону, Таганрог, 2020 - (140 с.) https://biblioclub.ru/index.php?page=book&id=612162.

5.2 Лицензионное и свободно распространяемое программное обеспечение:
1. Office / Российский пакет офисных программ;
2. Windows / Операционная система семейства Linux;
3. Acrobat Reader;
4. Scilab.

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. **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
	З-505, Лекционная аудитория каф. ВМСС	парта, стол преподавателя, стул, мультимедийный проектор, доска маркерная, компьютер персональный, мел, маркер, стилус
Учебные аудитории для проведения лабораторных занятий	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
	З-506, Учебно-исследовательская лаборатория цифровых технологий защиты информации каф. ВМСС	стол преподавателя, стул, компьютерная сеть с выходом в Интернет, мультимедийный проектор, экран, доска маркерная, лабораторный стенд, сервер, компьютер персональный, инвентарь специализированный
Учебные аудитории для проведения промежуточной аттестации	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
	З-505, Лекционная аудитория каф. ВМСС	парта, стол преподавателя, стул, мультимедийный проектор, доска маркерная, компьютер персональный,

		мел, маркер, стилус
Помещения для самостоятельной работы	НТБ-303, Лекционная аудитория	стол компьютерный, стул, стол письменный, вешалка для одежды, компьютерная сеть с выходом в Интернет, компьютер персональный, принтер, кондиционер
	З-601, Класс самостоятельных занятий каф. ВМСС	
Помещения для консультирования	З-302, Кабинет сотрудников каф. "ВМСС"	
Помещения для хранения оборудования и учебного инвентаря	З-300, Помещение для лабораторного инвентаря каф. ВМСС	

Приложение А

БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА ДИСЦИПЛИНЫ

Методы и средства защиты информации

(название дисциплины)

7 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:

КМ-1 Контроль посещения лекций №1-2 по курсу МСЗИ; Контроль выполнения лабораторной работы №1 по курсу МСЗИ (25%) (Лабораторная работа)

КМ-2 Контроль посещения лекций №3-4 по курсу МСЗИ; Контроль выполнения лабораторной работы №2 по курсу МСЗИ (25%) (Лабораторная работа)

КМ-3 Контроль посещения лекций №5-6 по курсу МСЗИ; Контроль выполнения лабораторной работы №3 по курсу МСЗИ (25%) (Лабораторная работа)

КМ-4 Контроль посещения лекций №7-8 по курсу МСЗИ; Контроль выполнения лабораторной работы №4 по курсу МСЗИ (25%) (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	Основы информационной безопасности: нормативные и технические аспекты					
1.1	Основы информационной безопасности: нормативные и технические аспекты		+			
2	Криптография и защита данных					
2.1	Криптография и защита данных			+		
3	Практические аспекты и современные угрозы					
3.1	Практические аспекты и современные угрозы				+	
4	Аудит и управление информационной безопасностью					
4.1	Аудит и управление информационной безопасностью					+
		Вес КМ, %:	25	25	25	25