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

Направление подготовки/специальность: 10.04.01 Информационная безопасность

Наименование образовательной программы: Управление информационной безопасностью

Уровень образования: высшее образование - магистратура

Форма обучения: Очная

Рабочая программа дисциплины
ТЕОРЕТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Блок:	**Блок 1 «Дисциплины (модули)»**
Часть образовательной программы:	**Часть, формируемая участниками образовательных отношений**
№ дисциплины по учебному плану:	**Б1.Ч.02**
Трудоемкость в зачетных единицах:	**3 семестр - 3;**
Часов (всего) по учебному плану:	**108 часов**
Лекции	**3 семестр - 32 часа;**
Практические занятия	**3 семестр - 32 часа;**
Лабораторные работы	**не предусмотрено учебным планом**
Консультации	**проводится в рамках часов аудиторных занятий**
Самостоятельная работа	**3 семестр - 43,7 часа;**
в том числе на КП/КР	**не предусмотрено учебным планом**
Иная контактная работа	**проводится в рамках часов аудиторных занятий**
включая: **Контрольная работа** **Тестирование**	
Промежуточная аттестация:	
Зачет с оценкой	**3 семестр - 0,3 часа;**

Москва 2026

ПРОГРАММУ СОСТАВИЛ:

Преподаватель	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Карпов Д.С. Идентификатор: R3575f0b9-KarpovDS-fe8a59b5	Д.С. Карпов

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Минзов А.С. Идентификатор: R17801759-MinzovAS-e8de8907	А.С. Минзов
Заведующий выпускающей кафедрой	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Невский А.Ю. Идентификатор: R4bc65573-NevskyAY-0b6e493d	А.Ю. Невский

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель освоения дисциплины: приобретение необходимых теоретических знаний и практических навыков по использованию принципов и методов защиты компьютерной информации, а также проектированию и анализу защищенных автоматизированных систем (АС).

Задачи дисциплины

- изучение принципов функционирования защищенных АС;
- освоение методов проектирования защищенных АС;
- приобретение навыков использования критериев и методов оценки защищенности АС.

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**
РПК-1 Способен активно участвовать в управлении функционированием системы обеспечения информационной безопасности (СОИБ) организации на основе современных положений СМИБ	ИД-2$_{РПК-1}$ Проводит анализ безопасности компьютерных систем	знать: - методологические основы обеспечения безопасности компьютерных систем; - требования к защищенности автоматизированных систем и информационных технологий; - угрозы и методы нарушения безопасности компьютерных систем. уметь: - проводить анализ автоматизированных систем с точки зрения обеспечения компьютерной безопасности; - использовать критерии оценки защищенности автоматизированных систем и информационных технологий.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к основной профессиональной образовательной программе Управление информационной безопасностью (далее – ОПОП), направления подготовки 10.04.01 Информационная безопасность, уровень образования: высшее образование - магистратура.

Базируется на уровне высшего образования (бакалавриат, специалитет).

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	Угрозы и способы нарушения компьютерной безопасности	22	3	8	-	8	-	-	-	-	-	6	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Угрозы и способы нарушения компьютерной безопасности"
1.1	Основные понятия курса	10		4	-	4	-	-	-	-	-	2	-	***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы
1.2	Каналы утечки информации в компьютерных системах	12		4	-	4	-	-	-	-	-	4	-	***Подготовка домашнего задания:*** Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Угрозы и способы нарушения компьютерной 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:

														Подготовка к практическим занятиям: Изучение материала по разделу "Угрозы и способы нарушения компьютерной безопасности" подготовка к выполнению заданий на практических занятиях ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Угрозы и способы нарушения компьютерной безопасности" ***Изучение материалов литературных источников:*** [3], 45-65 [5], 5-75 [6], 133-147
2	Теоретические основы построения систем аутентификации	34		12	-	12	-	-	-	-	-	10	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Теоретические основы построения систем аутентификации" ***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы ***Подготовка домашнего задания:*** Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Теоретические основы построения систем аутентификации" 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
2.1	Типы базового секрета и атаки на системы парольной аутентификации	10		4	-	4	-	-	-	-	-	2	-	
2.2	Принципы биометрической аутентификации	12		4	-	4	-	-	-	-	-	4	-	
2.3	Классификация устройств аутентификации	12		4	-	4	-	-	-	-	-	4	-	

														представляются в электронном виде или в форме распечатанных презентационных слайдов. В качестве тем докладов студентам предлагаются следующие варианты: ***<u>Подготовка к практическим занятиям:</u>*** Изучение материала по разделу "Теоретические основы построения систем аутентификации" подготовка к выполнению заданий на практических занятиях ***<u>Самостоятельное изучение теоретического материала:</u>*** Изучение дополнительного материала по разделу "Теоретические основы построения систем аутентификации" ***<u>Изучение материалов литературных источников:</u>*** [3], 5-65 [4], 114-117
3	Стандарты оценки защищенности компьютерных систем и информационных технологий	34		12	-	12	-	-	-	-	-	10	-	***<u>Подготовка к текущему контролю:</u>*** Повторение материала по разделу "Стандарты оценки защищенности компьютерных систем и информационных технологий"
3.1	Основные определения и требования к защищенности компьютерных систем	10		4	-	4	-	-	-	-	-	2	-	***<u>Подготовка к аудиторным занятиям:</u>*** Проработка лекции, выполнение и подготовка к защите лаб. работы ***<u>Подготовка домашнего задания:</u>*** Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Стандарты оценки защищенности компьютерных систем и информационных технологий" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам.
3.2	Состав и общая характеристика руководящих документов ФСТЭК России по защите информации от несанкционированного доступа	12		4	-	4	-	-	-	-	-	4	-	
3.3	Назначение и состав общих критериев оценки безопасности	12		4	-	4	-	-	-	-	-	4	-	

	информационных технологий													***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: ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Стандарты оценки защищенности компьютерных систем и информационных технологий" подготовка к выполнению заданий на практических занятиях ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Стандарты оценки защищенности компьютерных систем и информационных технологий" ***Изучение материалов литературных источников:*** [1], 157-178 [2], 147-168
	Зачет с оценкой	18.0		-	-	-	-	-	-	-	0.3	-	17.7	
	Всего за семестр	**108.0**		**32**	**-**	**32**	**-**	**-**	**-**	**-**	**0.3**	**26**	**17.7**	
	Итого за семестр	**108.0**		**32**	**-**	**32**	**-**		**-**		**0.3**	**43.7**		

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. Угрозы и способы нарушения компьютерной безопасности

1.1. Основные понятия курса

Цели угроз безопасности информации в компьютерных системах. Угрозы безопасности информации в компьютерных системах..

1.2. Каналы утечки информации в компьютерных системах

Способы нарушения безопасности информации в компьютерных системах..

2. Теоретические основы построения систем аутентификации

2.1. Типы базового секрета и атаки на системы парольной аутентификации

Защита от атак и оценка стойкости систем парольной аутентификации. Регистрация пользователей в системах парольной аутентификации. Энтропия при выборе пароля пользователя..

2.2. Принципы биометрической аутентификации

Создание и проверка биометрических эталонов. Оценка качества биометрической аутентификации. Использование криптографии в системах биометрической аутентификации..

2.3. Классификация устройств аутентификации

Генераторы одноразовых паролей. Использование PIN-кодов в устройствах аутентификации. Регистрация пользователей при применении устройств аутентификации..

3. Стандарты оценки защищенности компьютерных систем и информационных технологий

3.1. Основные определения и требования к защищенности компьютерных систем

Классы защищенности компьютерных систем в соответствии с TCSEC..

3.2. Состав и общая характеристика руководящих документов ФСТЭК России по защите информации от несанкционированного доступа

Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Показатели защищенности средств вычислительной техники от несанкционированного доступа к информации. Классификация подлежащих защите автоматизированных систем..

3.3. Назначение и состав общих критериев оценки безопасности информационных технологий

Представление и формирование требований безопасности. Функциональные требования безопасности. Требования доверия к безопасности..

3.3. Темы практических занятий

1. 1. Классификация угроз безопасности информации в компьютерных системах;
2. 4. Системы биометрической аутентификации;
3. 5. Системы аутентификации с использованием устройств;
4. 6. Требования стандарта Trusted Computer System Evaluation Criteria;
5. 7. Требования Руководящих документов ФСТЭК России по защите от

несанкционированного доступа к информации;
6. 8. Требования безопасности Общих критериев;
7. 2. Способы нарушения безопасности и каналы утечки информации в компьютерных системах;
8. 3. Системы парольной аутентификации и их анализ.

3.4. Темы лабораторных работ

не предусмотрено

3.5 Консультации

Групповые консультации по разделам дисциплины (ГК)

1. Обсуждение материалов по кейсам раздела "Угрозы и способы нарушения компьютерной безопасности"
2. Обсуждение материалов по кейсам раздела "Теоретические основы построения систем аутентификации"
3. Обсуждение материалов по кейсам раздела "Стандарты оценки защищенности компьютерных систем и информационных технологий"

Текущий контроль (ТК)

1. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Угрозы и способы нарушения компьютерной безопасности"
2. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Теоретические основы построения систем аутентификации"
3. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Стандарты оценки защищенности компьютерных систем и информационных технологий"

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:					
угрозы и методы нарушения безопасности компьютерных систем	ИД-2$_{РПК-1}$		+		Контрольная работа/Контрольная работа: практическое задание №2 «Принципы создания и использования устройств аутентификации» Тестирование/Тест №1 «Теоретические основы построения систем парольной и биометрической аутентификации пользователей»
требования к защищенности автоматизированных систем и информационных технологий	ИД-2$_{РПК-1}$			+	Тестирование/Тест №2 «Требования к безопасности компьютерных систем и информационных технологий». Презентация доклада
методологические основы обеспечения безопасности компьютерных систем	ИД-2$_{РПК-1}$	+			Контрольная работа/Контрольная работа: практическое задание №1 «Угрозы безопасности информации и каналы утечки информации»
Уметь:					
использовать критерии оценки защищенности автоматизированных систем и информационных технологий	ИД-2$_{РПК-1}$		+		Контрольная работа/Контрольная работа: практическое задание №2 «Принципы создания и использования устройств аутентификации» Тестирование/Тест №1 «Теоретические основы построения систем парольной и биометрической аутентификации пользователей»
проводить анализ автоматизированных систем с точки зрения обеспечения компьютерной безопасности	ИД-2$_{РПК-1}$			+	Тестирование/Тест №2 «Требования к безопасности компьютерных систем и информационных технологий». Презентация доклада

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

4.1. Текущий контроль успеваемости

3 семестр

Форма реализации: Письменная работа

1. Тест №1 «Теоретические основы построения систем парольной и биометрической аутентификации пользователей» (Тестирование)
2. Тест №2 «Требования к безопасности компьютерных систем и информационных технологий». Презентация доклада (Тестирование)

Форма реализации: Устная форма

1. Контрольная работа: практическое задание №1 «Угрозы безопасности информации и каналы утечки информации» (Контрольная работа)
2. Контрольная работа: практическое задание №2 «Принципы создания и использования устройств аутентификации» (Контрольная работа)

Балльно-рейтинговая структура дисциплины является приложением А.

4.2 Промежуточная аттестация по дисциплине

Зачет с оценкой (Семестр №3)

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

В диплом выставляется оценка за 3 семестр.

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

5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1 Печатные и электронные издания:

1. Грушо, А. А. Теоретические основы компьютерной безопасности : учебное пособие для вузов по специальности 090100 "Информационная безопасность" / А. А. Грушо, Э. А. Применко, Е. Е. Тимонина. – М. : АКАДЕМИЯ, 2009. – 272 с. – (Высшее профессиональное образование). – ISBN 978-5-7695-4242-8.;
2. 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.;
3. Хорев, П. Б. Программно-аппаратная защита информации : учебное пособие для вузов по направлению "Информационная безопасность" / П. Б. Хорев. – 2-е изд., испр. и доп. – М. : Форум : ИНФРА-М, 2017. – 352 с. – (Высшее образование). – ISBN 978-5-00091-004-7.;
4. Горбатов, В. С. Основы технологии PKI / В. С. Горбатов, О. Ю. Полянская. – М. : Горячая Линия-Телеком, 2004. – 248 с. – ISBN 5-935171-54-6.;
5. Теоретические основы компьютерной безопасности : Учебное пособие для вузов по специальности "Компьютерная безопасность", "Комплексное обеспечение информационной безопасности автоматизированных систем", "Информационная безопасность

телекоммуникационных систем" / П. Н. Девянин, и др. – М. : Радио и связь, 2000. – 192 с. – ISBN 5-256-01413-7.;
6. А. Щербаков- "Современная компьютерная безопасность. Теоретические основы. Практические аспекты", Издательство: "Книжный мир", Москва, 2009 - (352 с.) https://biblioclub.ru/index.php?page=book&id=89798.

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

5.3 Интернет-ресурсы, включая профессиональные базы данных и информационно-справочные системы:
1. **ЭБС Лань** - https://e.lanbook.com/
2. **Научная электронная библиотека** - https://elibrary.ru/
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. **Электронная библиотека МЭИ (ЭБ МЭИ)** - http://elib.mpei.ru/login.php
7. **Портал открытых данных Российской Федерации** - https://data.gov.ru
8. **База открытых данных Министерства труда и социальной защиты РФ** - https://rosmintrud.ru/opendata
9. **База открытых данных профессиональных стандартов Министерства труда и социальной защиты РФ** - http://profstandart.rosmintrud.ru/obshchiy-informatsionnyy-blok/natsionalnyy-reestr-professionalnykh-standartov/
10. **База открытых данных Министерства экономического развития РФ** - http://www.economy.gov.ru
11. **База открытых данных Росфинмониторинга** - http://www.fedsfm.ru/opendata
12. **Электронная открытая база данных "Polpred.com Обзор СМИ"** - https://www.polpred.com
13. **Национальный портал онлайн обучения «Открытое образование»** - https://openedu.ru
14. **Официальный сайт Федерального агентства по техническому регулированию и метрологии** - http://protect.gost.ru/
15. **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-301, Учебная аудитория	стол преподавателя, стол учебный, стул, мультимедийный проектор, экран, доска маркерная, кондиционер
	К-601, Учебная аудитория	парта со скамьей, стол преподавателя, стул, трибуна, доска меловая, мультимедийный проектор, экран
Учебные аудитории для проведения практических занятий, КР и КП	К-307, Учебная лаборатория "Открытое программное обеспечение"	стол преподавателя, стол компьютерный, стол учебный, стул, вешалка для одежды, тумба, компьютерная сеть с выходом в Интернет, мультимедийный проектор,

		экран, доска маркерная, сервер, компьютер персональный, кондиционер
Учебные аудитории для проведения промежуточной аттестации	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
	К-307, Учебная лаборатория "Открытое программное обеспечение"	стол преподавателя, стол компьютерный, стол учебный, стул, вешалка для одежды, тумба, компьютерная сеть с выходом в Интернет, мультимедийный проектор, экран, доска маркерная, сервер, компьютер персональный, кондиционер
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
	К-307, Учебная лаборатория "Открытое программное обеспечение"	стол преподавателя, стол компьютерный, стол учебный, стул, вешалка для одежды, тумба, компьютерная сеть с выходом в Интернет, мультимедийный проектор, экран, доска маркерная, сервер, компьютер персональный, кондиционер
	К-302, Учебная лаборатория "Информационно-аналитические технологии"	стол преподавателя, стол компьютерный, стул, мультимедийный проектор, экран, доска маркерная, сервер, компьютер персональный, кондиционер
Помещения для консультирования	К-301, Учебная аудитория	стол преподавателя, стол учебный, стул, мультимедийный проектор, экран, доска маркерная, кондиционер
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

Теоретические основы компьютерной безопасности

(название дисциплины)

3 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:

КМ-1 Контрольная работа: практическое задание №1 «Угрозы безопасности информации и каналы утечки информации» (Контрольная работа)

КМ-2 Тест №1 «Теоретические основы построения систем парольной и биометрической аутентификации пользователей» (Тестирование)

КМ-3 Контрольная работа: практическое задание №2 «Принципы создания и использования устройств аутентификации» (Контрольная работа)

КМ-4 Тест №2 «Требования к безопасности компьютерных систем и информационных технологий». Презентация доклада (Тестирование)

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	15
1	Угрозы и способы нарушения компьютерной безопасности					
1.1	Основные понятия курса		+			
1.2	Каналы утечки информации в компьютерных системах		+			
2	Теоретические основы построения систем аутентификации					
2.1	Типы базового секрета и атаки на системы парольной аутентификации			+	+	
2.2	Принципы биометрической аутентификации			+	+	
2.3	Классификация устройств аутентификации			+	+	
3	Стандарты оценки защищенности компьютерных систем и информационных технологий					
3.1	Основные определения и требования к защищенности компьютерных систем					+
3.2	Состав и общая характеристика руководящих документов ФСТЭК России по защите информации от несанкционированного доступа					+
3.3	Назначение и состав общих критериев оценки безопасности информационных технологий					+
	Вес КМ, %:		20	20	20	40