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
ЗАЩИЩЕННЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ

Блок:	**Блок 1 «Дисциплины (модули)»**
Часть образовательной программы:	**Базовая**
№ дисциплины по учебному плану:	**Б1.Б.01**
Трудоемкость в зачетных единицах:	**3 семестр - 4;**
Часов (всего) по учебному плану:	**144 часа**
Лекции	**3 семестр - 16 часов;**
Практические занятия	**3 семестр - 48 часа;**
Лабораторные работы	**не предусмотрено учебным планом**
Консультации	**3 семестр - 2 часа;**
Самостоятельная работа	**3 семестр - 77,5 часа;**
в том числе на КП/КР	**не предусмотрено учебным планом**
Иная контактная работа	**проводится в рамках часов аудиторных занятий**
включая: **Отчет**	
Промежуточная аттестация:	
Экзамен	**3 семестр - 0,5 часа;**

Москва 2020

ПРОГРАММУ СОСТАВИЛ:

Преподаватель	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Капгер И.В. Идентификатор: R5d33df1e-KapgerIV-059b09ee	И.В. Капгер
(должность)	(подпись)	(расшифровка подписи)

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
(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: приобретение необходимых теоретических знаний и практических навыков по созданию и эксплуатации защищенных информационных систем

Задачи дисциплины

- изучение методов анализа защищенности информационных систем;
- освоение способов выбора и настройки программно-аппаратных средств защиты информационных систем;
- приобретение навыков построения и использования инфраструктуры открытых ключей в защищенных информационных системах.

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

Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**	**Запланированные результаты обучения**
ОПК-1 способностью к коммуникации в устной и письменной формах на государственном и одном из иностранных языков для решения задач профессиональной деятельности		знать: - формальные модели, лежащие в основе защищенных информационных систем.
ПК-1 способностью анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты		уметь: - проводить анализ информационных систем с точки зрения обеспечения их защищенности.
ПК-3 способностью проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов		уметь: - выбирать методы защиты информации при ее передаче по открытым компьютерным сетям.
ПК-4 способностью разрабатывать программы		знать: - каналы распространения вредоносных

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Запланированные результаты обучения
и методики испытаний средств и систем обеспечения информационной безопасности		программ, способы предупреждения заражения вредоносными программами и методы их обнаружения.
ПК-7 способностью проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента		уметь: - использовать формальные модели построения защищенных информационных систем.
ПК-8 способностью обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи		уметь: - применять методы и программно-аппаратные средства защиты информационных систем.
ПК-10 способностью проводить аттестацию объектов информатизации по требованиям безопасности информации		знать: - угрозы информационной безопасности при подключении информационной системы к глобальной компьютерной сети.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

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

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	Модели и критерии оценки защищенных информационных систем	14	3	2	-	4	-	-	-	-	-	8	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Модели и критерии оценки защищенных информационных систем"
1.1	Тема 1. Критерии оценки защищенных информационных систем	7		1	-	2	-	-	-	-	-	4	-	***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 "Модели и критерии оценки защищенных информационных систем" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам. ***Подготовка к контрольной работе:*** Изучение материалов по разделу Модели и критерии оценки защищенных информационных систем и подготовка к контрольной работе ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Модели и критерии оценки защищенных информационных систем" подготовка к
1.2	Тема 2. Угрозы информационной безопасности	7		1	-	2	-	-	-	-	-	4	-	

														выполнению заданий на практических занятиях ***<u>Самостоятельное изучение теоретического материала:</u>*** Изучение дополнительного материала по разделу "Модели и критерии оценки защищенных информационных систем" ***<u>Изучение материалов литературных источников:</u>*** [3], 104-156 [4], 1-227 [6], 6-40
2	Программно-аппаратные средства защищенных информационных систем	52		10	-	22	-	-	-	-	-	20	-	***<u>Подготовка к текущему контролю:</u>*** Повторение материала по разделу "Программно-аппаратные средства защищенных информационных систем" ***<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 "Программно-аппаратные средства защищенных информационных систем" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам. ***<u>Подготовка к контрольной работе:</u>*** Изучение материалов по разделу Программно-аппаратные средства защищенных информационных систем и подготовка к контрольной работе ***<u>Подготовка к практическим занятиям:</u>*** Изучение материала по разделу "Программно-аппаратные средства
2.1	Тема 3. Классификация программно-аппаратных средств защиты ИС.	10		2	-	4	-	-	-	-	-	4	-	
2.2	Тема 4. Принципы работы межсетевых экранов.	8		2	-	2	-	-	-	-	-	4	-	
2.3	Тема 5. Сканеры уязвимостей информационных систем.	10		2	-	4	-	-	-	-	-	4	-	
2.4	Тема 6. Системы защиты от утечек данных (DLP-системы).	12		2	-	6	-	-	-	-	-	4	-	
2.5	Тема 7. Вредоносные программы, их признаки и классификация.	12		2	-	6	-	-	-	-	-	4	-	

														защищенных информационных систем" подготовка к выполнению заданий на практических занятиях ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Программно-аппаратные средства защищенных информационных систем" ***Изучение материалов литературных источников:*** [2], 1-352
3	Инфраструктура открытых ключей в защищенных информационных системах	42		4	-	22	-	-	-	-	-	16	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Инфраструктура открытых ключей в защищенных информационных системах" ***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 "Инфраструктура открытых ключей в защищенных информационных системах" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам. ***Подготовка к контрольной работе:*** Изучение материалов по разделу Инфраструктура открытых ключей в защищенных информационных системах и подготовка к контрольной работе ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Инфраструктура открытых ключей в защищенных информационных системах"
3.1	Тема 8. Принципы аутентификации на основе модели «рукопожатия».	9		1	-	4	-	-	-	-	-	4	-	
3.2	Тема 9. Использование асимметричной криптографии в системах аутентификации.	11		1	-	6	-	-	-	-	-	4	-	
3.3	Тема 10. Отзыв сертификатов, его причины и стратегии	11		1	-	6	-	-	-	-	-	4	-	
3.4	Тема 11. Способы хранения личных (закрытых) ключей.	11		1	-	6	-	-	-	-	-	4	-	

														подготовка к выполнению заданий на практических занятиях ***<u>Самостоятельное изучение теоретического материала:</u>*** Изучение дополнительного материала по разделу "Инфраструктура открытых ключей в защищенных информационных системах" ***<u>Изучение материалов литературных источников:</u>*** [1], 50-87 [5], 1-88
	Экзамен	36.0		-	-	-	-	2	-	-	0.5	-	33.5	
	Всего за семестр	**144.0**		**16**	**-**	**48**	**-**	**2**	**-**	**-**	**0.5**	**44**	**33.5**	
	Итого за семестр	**144.0**		**16**	**-**	**48**	**2**		**-**		**0.5**	**77.5**		

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. Модели и критерии оценки защищенных информационных систем

1.1. Тема 1. Критерии оценки защищенных информационных систем

Определение защищенной информационной системы (ИС), критерии оценки защищенности ИС. Методология анализа защищенности ИС.

1.2. Тема 2. Угрозы информационной безопасности

Основные угрозы информационной безопасности при подключении ИС к сети Интернет..

2. Программно-аппаратные средства защищенных информационных систем

2.1. Тема 3. Классификация программно-аппаратных средств защиты ИС.

Классификация межсетевых экранов, сканеров безопасности, фильтрующих маршрутизаторов и систем DLP..

2.2. Тема 4. Принципы работы межсетевых экранов.

Настройка и использование межсетевых экранов..

2.3. Тема 5. Сканеры уязвимостей информационных систем.

Системы обнаружения атак. Системы контроля содержимого..

2.4. Тема 6. Системы защиты от утечек данных (DLP-системы).

Назначение, архитектура и порядок функционирования DLP-систем..

2.5. Тема 7. Вредоносные программы, их признаки и классификация.

Каналы распространения и предупреждение заражения вредоносными программами. Методы обнаружения и удаления вредоносных программ..

3. Инфраструктура открытых ключей в защищенных информационных системах

3.1. Тема 8. Принципы аутентификации на основе модели «рукопожатия».

Построение системы аутентификации на основе аппаратных и программных генераторов одноразовых паролей. Использование непрямой аутентификации..

3.2. Тема 9. Использование асимметричной криптографии в системах аутентификации.

Управление сертификатами открытых ключей. Структура и разновидности сертификатов. Элементы инфраструктуры открытых ключей (PKI). Архитектура PKI..

3.3. Тема 10. Отзыв сертификатов, его причины и стратегии

Списки отозванных сертификатов, их структура и виды. Распространение сертификатов и списков отозванных сертификатов. Управление жизненным циклом сертификатов..

3.4. Тема 11. Способы хранения личных (закрытых) ключей.

Управление доступом к устройству с личным ключом. Хранение личных ключей на сервере..

3.3. Темы практических занятий

1. 1. Модели и критерии оценки защищенности информационных систем;
2. 2. Выполнение практического задания №1 «Межсетевые экраны»;
3. 3. Программно-аппаратные средства защиты информационных;
4. 4. Защита отчета о выполнении практического задания №;
5. 5. Методы выбора, настройки и использования межсетевых кранов;
6. 6. Выполнение практического задания №2 «Сканеры уязвимостей информационных систем»;
7. 7. Анализ защищенности информационных систем с использованием сканеров уязвимостей;
8. 8. Защита отчета о выполнении практического задания №2;
9. 9. Использование систем защиты от утечек данных в информационных системах;
10. 10. Выполнение практического задания №3 «Средства работы с сертификатами и защиты от вредоносных программ»;
11. 11. Элементы и архитектура удостоверяющих центров в инфраструктуре открытых ключей;
12. 12. Защита отчета о выполнении практического задания №3;
13. 13. Управление распространением и жизненным циклом сертификатов открытых ключей в защищенных информационных системах;
14. 14. Выполнение практического задания №4 «Системы защиты от утечек данных и контроля содержимого»;
15. 15. Способы хранения личных ключей пользователей в инфраструктуре открытых ключей;
16. 16. Защита отчета о выполнении практического задания №4.

3.4. Темы лабораторных работ

не предусмотрено

3.5 Консультации

Групповые консультации по разделам дисциплины (ГК)

1. Обсуждение материалов по кейсам раздела "Модели и критерии оценки защищенных информационных систем"
2. Обсуждение материалов по кейсам раздела "Программно-аппаратные средства защищенных информационных систем"
3. Обсуждение материалов по кейсам раздела "Инфраструктура открытых ключей в защищенных информационных системах"

Текущий контроль (ТК)

1. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Модели и критерии оценки защищенных информационных систем"
2. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Программно-аппаратные средства защищенных информационных систем"
3. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Инфраструктура открытых ключей в защищенных информационных системах"

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:					
формальные модели, лежащие в основе защищенных информационных систем	ОПК-1(Компетенция)	+			Отчет/Защита практического задания №1 «Межсетевые экраны»
каналы распространения вредоносных программ, способы предупреждения заражения вредоносными программами и методы их обнаружения	ПК-4(Компетенция)		+		Отчет/Защита практического задания №3 «Средства работы с сертификатами и защиты от вредоносных программ»
угрозы информационной безопасности при подключении информационной системы к глобальной компьютерной сети	ПК-10(Компетенция)	+			Отчет/Защита практического задания №1 «Межсетевые экраны»
Уметь:					
проводить анализ информационных систем с точки зрения обеспечения их защищенности	ПК-1(Компетенция)		+		Отчет/Защита практического задания №3 «Средства работы с сертификатами и защиты от вредоносных программ»
выбирать методы защиты информации при ее передаче по открытым компьютерным сетям	ПК-3(Компетенция)			+	Отчет/Защита практического задания №4 «Системы защиты от утечек данных и контроля содержимого». Тест №2 «Методы построения и использования инфраструктуры открытых ключей»
использовать формальные модели построения защищенных информационных систем	ПК-7(Компетенция)		+		Отчет/Защита практического задания №1 «Межсетевые экраны»
применять методы и программно-аппаратные средства защиты информационных систем	ПК-8(Компетенция)		+		Отчет/Защита практического задания №2 «Сканеры уязвимостей».Тест №1 «Модели защищенных информационных систем. Выбор программно-аппаратных средств защиты в информационных

					системах»

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. Защита практического задания №1 «Межсетевые экраны» (Отчет)
2. Защита практического задания №2 «Сканеры уязвимостей».Тест №1 «Модели защищенных информационных систем. Выбор программно-аппаратных средств защиты в информационных системах» (Отчет)
3. Защита практического задания №3 «Средства работы с сертификатами и защиты от вредоносных программ» (Отчет)
4. Защита практического задания №4 «Системы защиты от утечек данных и контроля содержимого». Тест №2 «Методы построения и использования инфраструктуры открытых ключей» (Отчет)

Балльно-рейтинговая структура дисциплины является приложением А.

4.2 Промежуточная аттестация по дисциплине

Экзамен (Семестр №3)

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. Горбатов, В. С. Основы технологии PKI / В. С. Горбатов, О. Ю. Полянская . – М. : Горячая Линия-Телеком, 2004 . – 248 с. - ISBN 5-935171-54-6 .;
2. 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 .;
3. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие по направлению "Прикладная информатика" / Е. К. Баранова, А. В. Бабаш . – 3-е изд., перераб. и доп . – М. : РИОР : ИНФРА-М, 2017 . – 322 с. – (Высшее образование) . - ISBN 978-5-369-01450-9 .;
4. 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 .;
5. Хорев, П. Б. Криптографические протоколы : учебное пособие 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") . – М. : Изд-во МЭИ, 2019 . – 88 с. - ISBN 978-5-7046-2162-1 . http://elib.mpei.ru/action.php?kt_path_info=ktcore.SecViewPlugin.actions.document&fDocumentId=10969;

6. Бахаров Л. Е.- "Информационная безопасность и защита информации (разделы криптография и стеганография)", Издательство: "МИСИС", Москва, 2019 - (59 с.) https://e.lanbook.com/book/116907.

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. **Электронные ресурсы издательства Springer** - https://link.springer.com/
5. **База данных Scopus** - http://www.scopus.com
6. **ЭБС "Консультант студента"** - http://www.studentlibrary.ru/
7. **Журнал Science** - https://www.sciencemag.org/
8. **Электронная библиотека МЭИ (ЭБ МЭИ)** - http://elib.mpei.ru/login.php
9. **Информационно-справочная система «Кодекс/Техэксперт»** - Http:\\proinfosoft.ru; http://docs.cntd.ru/
10. **Федеральный портал "Российское образование"** - http://www.edu.ru

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Тип помещения	Номер аудитории, наименование	Оснащение
Учебные аудитории для проведения лекционных занятий и текущего контроля	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-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
	А-307, Аудитория для проведения практических занятий	стол преподавателя, стол, стул, доска меловая
Помещения для самостоятельной	НТБ-303, Компьютерный	стол компьютерный, стул, стол письменный, вешалка для одежды,

работы	читальный зал	компьютерная сеть с выходом в Интернет, компьютер персональный, принтер, кондиционер
Помещения для консультирования	А-307, Аудитория для проведения практических занятий	стол преподавателя, стол, 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

Защищенные информационные системы

(название дисциплины)

3 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:

КМ-1 Защита практического задания №1 «Межсетевые экраны» (Отчет)

КМ-2 Защита практического задания №2 «Сканеры уязвимостей».Тест №1 «Модели защищенных информационных систем. Выбор программно-аппаратных средств защиты в информационных системах» (Отчет)

КМ-3 Защита практического задания №3 «Средства работы с сертификатами и защиты от вредоносных программ» (Отчет)

КМ-4 Защита практического задания №4 «Системы защиты от утечек данных и контроля содержимого». Тест №2 «Методы построения и использования инфраструктуры открытых ключей» (Отчет)

Вид промежуточной аттестации – Экзамен.

Номер раздела	Раздел дисциплины	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
		Неделя КМ:	4	8	12	15
1	Модели и критерии оценки защищенных информационных систем					
1.1	Тема 1. Критерии оценки защищенных информационных систем		+			
1.2	Тема 2. Угрозы информационной безопасности		+			
2	Программно-аппаратные средства защищенных информационных систем					
2.1	Тема 3. Классификация программно-аппаратных средств защиты ИС.		+			
2.2	Тема 4. Принципы работы межсетевых экранов.			+		
2.3	Тема 5. Сканеры уязвимостей информационных систем.			+		
2.4	Тема 6. Системы защиты от утечек данных (DLP-системы).			+	+	
2.5	Тема 7. Вредоносные программы, их признаки и классификация.				+	
3	Инфраструктура открытых ключей в защищенных информационных системах					
3.1	Тема 8. Принципы аутентификации на основе модели «рукопожатия».					+
3.2	Тема 9. Использование асимметричной криптографии в системах аутентификации.					+

3.3	Тема 10. Отзыв сертификатов, его причины и стратегии				+
3.4	Тема 11. Способы хранения личных (закрытых) ключей.				+
	Вес КМ, %:	25	25	25	25