

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
МЕТОДЫ И СРЕДСТВА КОНТРОЛЯ ЭФФЕКТИВНОСТИ ЗАЩИТЫ
ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Блок:	Блок 1 «Дисциплины (модули)»
Часть образовательной программы:	Часть, формируемая участниками образовательных отношений
№ дисциплины по учебному плану:	Б4.Ч.03
Трудоемкость в зачетных единицах:	3 семестр - 2;
Часов (всего) по учебному плану:	72 часа
Лекции	3 семестр - 16 часов;
Практические занятия	не предусмотрено учебным планом
Лабораторные работы	не предусмотрено учебным планом
Консультации	проводится в рамках часов аудиторных занятий
Самостоятельная работа	3 семестр - 55,7 часа;
в том числе на КП/КР	не предусмотрено учебным планом
Иная контактная работа	проводится в рамках часов аудиторных занятий
включая:	
Тестирование	
Промежуточная аттестация:	
Зачет	3 семестр - 0,3 часа;

Москва 2024

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


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: формирование у обучаемых знаний о современных задачах, методах и средствах защиты информации от несанкционированного доступа, принципах построения систем защиты от угрозы нарушения конфиденциальности, целостности и доступности информации, основные виды политик безопасности, технологии аутентификации, защиты межсетевое взаимодействия, обнаружения вторжений и защиты от вирусов

Задачи дисциплины

- представить студентам необходимые знания по определению эффективности защиты от угроз информационной безопасности, определению оптимальных методов борьбы с нарушениями, по составлению политики безопасности информационной системы предприятия, дать сведения по проектированию систем анализа безопасности компьютерных сетей и систем.

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	<p>знать:</p> <ul style="list-style-type: none">- современную классификацию средств защиты информации в корпоративных вычислительных сетях и системах;- инструментальные программные и аппаратные средства анализа защищенности информационных систем и сетей;- этапы и технологию проектирования и создания безопасных информационных систем;- современные технологии построения безопасных информационных систем. <p>уметь:</p> <ul style="list-style-type: none">- работать с основными программными и аппаратными средствами анализа защиты информационных систем;- использовать современные аппаратные средства анализа защиты информационных процессов в компьютерных системах;- разрабатывать структуру защищенной информационной системы;- использовать современные программные средства защиты информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к факультативным дисциплинам 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 2 зачетных единицы, 72 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	Критерии безопасности компьютерных систем США и Европы	32	3	6	-	-	-	-	-	-	-	26	-	<p><u>Подготовка к аудиторным занятиям:</u> Проработка лекции, выполнение и подготовка к защите лаб. работы</p> <p><u>Подготовка домашнего задания:</u> Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Критерии безопасности компьютерных систем США и Европы" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам.</p> <p><u>Подготовка к контрольной работе:</u> Изучение материалов по разделу Критерии безопасности компьютерных систем США и Европы и подготовка к контрольной работе</p> <p><u>Подготовка к практическим занятиям:</u> Изучение материала по разделу "Критерии безопасности компьютерных систем США и Европы" подготовка к выполнению заданий на практических занятиях</p> <p><u>Самостоятельное изучение теоретического материала:</u> Изучение дополнительного материала по разделу "Критерии безопасности компьютерных систем США и Европы"</p>	
1.1	Классификация методов и механизмов обеспечения компьютерной безопасности	14		2	-	-	-	-	-	-	-	-	12		-
1.2	Критерии безопасности компьютерных систем министерства обороны США («Оранжевая книга»)	18		4	-	-	-	-	-	-	-	-	14		-

													систем США и Европы" <u>Подготовка к текущему контролю:</u> Повторение материала по разделу "Критерии безопасности компьютерных систем США и Европы" <u>Изучение материалов литературных источников:</u> [1], 10-24
2	Модели и механизмы информационной безопасности	39.7	10	-	-	-	-	-	-	-	29.7	-	<u>Самостоятельное изучение теоретического материала:</u> Изучение дополнительного материала по разделу "Модели и механизмы информационной безопасности"
2.1	Модели и теоремы безопасности на основе дискреционной политики	8	2	-	-	-	-	-	-	-	6	-	<u>Подготовка к текущему контролю:</u> Повторение материала по разделу "Модели и механизмы информационной безопасности"
2.2	Модели и теоремы безопасности на основе мандатной политики	8	2	-	-	-	-	-	-	-	6	-	<u>Подготовка к аудиторным занятиям:</u> Проработка лекции, выполнение и подготовка к защите лаб. работы
2.3	Модели безопасности на основе ролевой политики	8	2	-	-	-	-	-	-	-	6	-	<u>Подготовка домашнего задания:</u> Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Модели и механизмы информационной безопасности" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам.
2.4	Понятие и разновидности скрытых каналов утечки информации в компьютерных системах	8	2	-	-	-	-	-	-	-	6	-	<u>Подготовка к контрольной работе:</u> Изучение материалов по разделу Модели и механизмы информационной безопасности и подготовка к контрольной работе
2.5	Модели и механизмы обеспечения целостности данных в компьютерных системах	7.7	2	-	-	-	-	-	-	-	5.7	-	<u>Подготовка к практическим занятиям:</u> Изучение материала по разделу "Модели и механизмы информационной безопасности" подготовка к выполнению заданий на

													практических занятиях <u>Изучение материалов литературных источников:</u> [1], 82-145 [2], 1-32
	Зачет	0.3	-	-	-	-	-	-	-	0.3	-	-	
	Всего за семестр	72.0	16	-	-	-	-	-	-	0.3	55.7	-	
	Итого за семестр	72.0	16	-	-	-	-	-	-	0.3	55.7	-	

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. Критерии безопасности компьютерных систем США и Европы

1.1. Классификация методов и механизмов обеспечения компьютерной безопасности
Понятие угроз безопасности, основы их классификации. Понятие политики безопасности в компьютерных системах и ее формализованное выражение в моделях безопасности.

1.2. Критерии безопасности компьютерных систем министерства обороны США («Оранжевая книга»)

Европейские критерии безопасности информационных технологий. Федеральные критерии безопасности информационных технологий Национального института стандартов и техно-логий и Агентства национальной безопасности США.

2. Модели и механизмы информационной безопасности

2.1. Модели и теоремы безопасности на основе дискреционной политики

Модели и теоремы безопасности на основе дискреционной политики (пятерное пространство Хартсона, модель на основе матрицы доступа), модели исследования распространения прав доступа в системах с дискреционной политикой (модель Харисона-Руizzo-Ульмана, модель типизованной матрицы доступа, модель TAKE-GRANT, расширенная модель TAKE-GRANT). Недостатки моделей дискреционного доступа, сценарий атаки "троянскими программами". Модели и теоремы безопасности на основе мандатной политики (модели Белла-ЛаПадулы, МакЛина, модель Low-WaterMark).

2.2. Модели и теоремы безопасности на основе мандатной политики

Модели и теоремы безопасности на основе мандатной политики (модели Белла-ЛаПадулы, МакЛина, модель Low-WaterMark).

2.3. Модели безопасности на основе ролевой политики

Модели безопасности на основе ролевой политики и технологии рабочих групп пользователей..

2.4. Понятие и разновидности скрытых каналов утечки информации в компьютерных системах

Понятие и разновидности скрытых каналов утечки информации в компьютерных системах, теоретико-вероятностные основы их выявления и нейтрализации (автоматная модель Гогена-Мессигера).

2.5. Модели и механизмы обеспечения целостности данных в компьютерных системах

Модели и механизмы обеспечения целостности данных в компьютерных системах (дискреционная модель Кларка-Вильсона, мандатная модель Кена Биба, технологии и протоколы выполнения транзакций в клиент-серверных системах).

3.3. Темы практических занятий

не предусмотрено

3.4. Темы лабораторных работ

не предусмотрено

3.5 Консультации

Групповые консультации по разделам дисциплины (ГК)

1. Обсуждение материалов по кейсам раздела "Критерии безопасности компьютерных систем США и Европы"
2. Обсуждение материалов по кейсам раздела "Модели и механизмы информационной безопасности"

Текущий контроль (ТК)

1. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Критерии безопасности компьютерных систем США и Европы"
2. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Модели и механизмы 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	
Знать:				
современные технологии построения безопасных информационных систем	ИД-2РПК-1		+	Тестирование/Тест № 3 «Классификация АС и требования по ЗИ (РД ГТК при Президенте РФ)». Контрольная работа №3. Оценка уровня защищенности СЗИ организации (банка) от НСД
этапы и технологию проектирования и создания безопасных информационных систем	ИД-2РПК-1	+		Тестирование/Тест №2 «Концепция защиты СВТ и АС от НСД (РД ГТК при Президенте РФ)». Контрольная работа №2. Разработка системы защиты информации организации (банка) от НСД
инструментальные программные и аппаратные средства анализа защищенности информационных систем и сетей	ИД-2РПК-1		+	Тестирование/Тест № 4 «Показатели защищенности СВТ от НСД к информации (РД ГТК при Президенте РФ)». Контрольная работа №4. Оценка уровня защищенности СЗИ организации (банка) с применением методики оценки информационных рисков и имитационного моделирования
современную классификацию средств защиты информации в корпоративных вычислительных сетях и системах	ИД-2РПК-1	+		Тестирование/Тест №1 «Общие сведения в предметной области дисциплины». Контрольная работа №1. Стандартные механизмы защиты СВТ от НСД на основе современной ОС типа Linux
Уметь:				
использовать современные программные средства защиты информации	ИД-2РПК-1		+	Тестирование/Тест № 3 «Классификация АС и требования по ЗИ (РД ГТК при Президенте РФ)». Контрольная работа №3. Оценка уровня защищенности СЗИ организации (банка) от НСД Тестирование/Тест № 4 «Показатели защищенности СВТ от НСД к информации (РД ГТК при Президенте РФ)». Контрольная работа №4. Оценка уровня защищенности СЗИ организации (банка) с применением методики оценки информационных рисков и имитационного моделирования
разрабатывать структуру	ИД-2РПК-1	+		Тестирование/Тест №2 «Концепция защиты СВТ и АС от НСД (РД

защищенной информационной системы				ГТК при Президенте РФ)». Контрольная работа №2. Разработка системы защиты информации организации (банка) от НСД
использовать современные аппаратные средства анализа защиты информационных процессов в компьютерных системах	ИД-2РПК-1	+		Тестирование/Тест №1 «Общие сведения в предметной области дисциплины». Контрольная работа №1. Стандартные механизмы защиты СВТ от НСД на основе современной ОС типа Linux
работать с основными программными и аппаратными средствами анализа защиты информационных систем	ИД-2РПК-1		+	Тестирование/Тест № 3 «Классификация АС и требования по ЗИ (РД ГТК при Президенте РФ)». Контрольная работа №3. Оценка уровня защищенности СЗИ организации (банка) от НСД Тестирование/Тест № 4 «Показатели защищенности СВТ от НСД к информации (РД ГТК при Президенте РФ)». Контрольная работа №4. Оценка уровня защищенности СЗИ организации (банка) с применением методики оценки информационных рисков и имитационного моделирования

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: Компьютерное задание

1. Тест № 3 «Классификация АС и требования по ЗИ (РД ГТК при Президенте РФ)». Контрольная работа №3. Оценка уровня защищенности СЗИ организации (банка) от НСД (Тестирование)
2. Тест № 4 «Показатели защищенности СВТ от НСД к информации (РД ГТК при Президенте РФ)». Контрольная работа №4. Оценка уровня защищенности СЗИ организации (банка) с применением методики оценки информационных рисков и имитационного моделирования (Тестирование)
3. Тест №1 «Общие сведения в предметной области дисциплины». Контрольная работа №1. Стандартные механизмы защиты СВТ от НСД на основе современной ОС типа Linux (Тестирование)
4. Тест №2 «Концепция защиты СВТ и АС от НСД (РД ГТК при Президенте РФ)». Контрольная работа №2. Разработка системы защиты информации организации (банка) от НСД (Тестирование)

Балльно-рейтинговая структура дисциплины является приложением А.

4.2 Промежуточная аттестация по дисциплине

Зачет (Семестр №3)

Оценка определяется в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ» на основании семестровой и зачетных составляющих.

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. Марков, А. С. Методы оценки несоответствия средств защиты информации / А. С. Марков, В. Л. Цирлов, А. В. Барабанов ; ред. А. С. Марков . – М. : Радио и связь, 2012 . – 192 с. - ISBN 5-89776-015-2 .;
2. Бондаренко И. С., Демчишин Ю. В.- "Методы и средства защиты информации", Издательство: "МИСИС", Москва, 2018 - (32 с.)
<https://e.lanbook.com/book/115269>.

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	М-511, Учебная аудитория	парта, стол преподавателя, стул, мультимедийный проектор, экран, доска маркерная, компьютер персональный
	К-601, Учебная аудитория	парта со скамьей, стол преподавателя, стул, трибуна, доска меловая, мультимедийный проектор, экран
Учебные аудитории для проведения промежуточной аттестации	М-511, Учебная аудитория	парта, стол преподавателя, стул, мультимедийный проектор, экран, доска маркерная, компьютер персональный
	Ж-120, Машинный зал ИВЦ	сервер, 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
	К-303, Учебная лаборатория "Программно-аппаратная защита информации"	стол преподавателя, стол компьютерный, стол учебный, стул, вешалка для одежды, компьютерная сеть с выходом в Интернет, компьютер персональный, кондиционер, телевизор
	К-307, Учебная лаборатория "Открытое"	стол преподавателя, стол компьютерный, стол учебный, стул, вешалка для одежды, тумба, компьютерная сеть с выходом в

	программное обеспечение"	Интернет, мультимедийный проектор, экран, доска маркерная, сервер, компьютер персональный, кондиционер
Помещения для консультирования	М-511, Учебная аудитория	парта, стол преподавателя, стул, мультимедийный проектор, экран, доска маркерная, компьютер персональный
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

БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА ДИСЦИПЛИНЫ

Методы и средства контроля эффективности защиты информации от несанкционированного доступа

(название дисциплины)

3 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:

- КМ-1 Тест №1 «Общие сведения в предметной области дисциплины». Контрольная работа №1. Стандартные механизмы защиты СВТ от НСД на основе современной ОС типа Linux (Тестирование)
- КМ-2 Тест №2 «Концепция защиты СВТ и АС от НСД (РД ГТК при Президенте РФ)». Контрольная работа №2. Разработка системы защиты информации организации (банка) от НСД (Тестирование)
- КМ-3 Тест №3 «Классификация АС и требования по ЗИ (РД ГТК при Президенте РФ)». Контрольная работа №3. Оценка уровня защищенности СЗИ организации (банка) от НСД (Тестирование)
- КМ-4 Тест №4 «Показатели защищенности СВТ от НСД к информации (РД ГТК при Президенте РФ)». Контрольная работа №4. Оценка уровня защищенности СЗИ организации (банка) с применением методики оценки информационных рисков и имитационного моделирования (Тестирование)

Вид промежуточной аттестации – Зачет.

Номер раздела	Раздел дисциплины	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
		Неделя КМ:	4	8	12	15
1	Критерии безопасности компьютерных систем США и Европы					
1.1	Классификация методов и механизмов обеспечения компьютерной безопасности		+	+		
1.2	Критерии безопасности компьютерных систем министерства обороны США («Оранжевая книга»)		+	+		
2	Модели и механизмы информационной безопасности					
2.1	Модели и теоремы безопасности на основе дискреционной политики				+	+
2.2	Модели и теоремы безопасности на основе мандатной политики				+	+
2.3	Модели безопасности на основе ролевой политики				+	+
2.4	Понятие и разновидности скрытых каналов утечки информации в компьютерных системах				+	+
2.5	Модели и механизмы обеспечения целостности данных в компьютерных системах				+	+
Вес КМ, %:			25	25	25	25