

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: Технологии разработки программного обеспечения

Уровень образования: высшее образование - бакалавриат

Форма обучения: Заочная

Рабочая программа дисциплины
МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ


Блок:	Блок 1 «Дисциплины (модули)»
Часть образовательной программы:	Вариативная
№ дисциплины по учебному плану:	Б1.В.01.06
Трудоемкость в зачетных единицах:	6 семестр - 5;
Часов (всего) по учебному плану:	180 часов
Лекции	6 семестр - 8 часов;
Практические занятия	6 семестр - 12 часов;
Лабораторные работы	не предусмотрено учебным планом
Консультации	6 семестр - 2 часа;
Самостоятельная работа	6 семестр - 156,2 часа;
в том числе на КП/КР	не предусмотрено учебным планом
Иная контактная работа	6 семестр - 1,5 часа;
включая: Тестирование Лабораторная работа	
Промежуточная аттестация:	
Экзамен	6 семестр - 0,3 часа;

Москва 2017

ПРОГРАММУ СОСТАВИЛ:

Преподаватель

(должность)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Баронов О.Р.
	Идентификатор	R90d76356-BaronovOR-7bf8fd7e

(подпись)


О.Р. Баронов

(расшифровка подписи)

СОГЛАСОВАНО:

Руководитель образовательной программы

(должность, ученая степень, ученое звание)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Вишняков С.В.
	Идентификатор	R35b26072-VishniakovSV-02810d9


(подпись)

С.В. Вишняков

(расшифровка подписи)

Заведующий выпускающей кафедры

(должность, ученая степень, ученое звание)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Вишняков С.В.
	Идентификатор	R35b26072-VishniakovSV-02810d9

(подпись)

С.В. Вишняков

(расшифровка подписи)

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель освоения дисциплины: Приобретение студентами теоретических знаний и практических навыков в области обеспечения информационной безопасности компьютерных систем и сетей

Задачи дисциплины

- Ознакомить обучающихся с общей постановкой задачи обеспечения информационной безопасности компьютерных систем и сетей и классификацией методов ее решения;
- Представить обучающимся способы идентификации и аутентификации субъектов компьютерных систем и сетей и разграничения их доступа к данным;
- Научить обучающихся выбирать (разрабатывать) и использовать конкретные программно-аппаратные средства защиты данных и безопасные информационные технологии;
- Научить обучающихся методам построения и использования симметричных и асимметричных криптографических 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
ПК-3 способностью обосновывать принимаемые проектные решения, осуществлять постановку и выполнять эксперименты по проверке их корректности и эффективности		знать: - способы построения симметричных и асимметричных криптографических систем; - методы разграничения полномочий пользователей и управления доступом к ресурсам в компьютерных системах и сетях. уметь: - использовать методы и средства криптографической защиты информации; - анализировать, выбирать и применять методы и средства защиты от вредоносных программ; - применять методы разграничения полномочий пользователей и управления доступом к данным в компьютерных системах и сетях.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к части, формируемой участниками образовательных отношений блока дисциплин основной профессиональной образовательной программе Технологии разработки программного обеспечения (далее – ОПОП), направления подготовки 09.03.01 Информатика и вычислительная техника, уровень образования: высшее образование - бакалавриат.

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 5 зачетных единиц, 180 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	Комплексный подход к обеспечению информационной безопасности	19.56	6	1.5	-	1.5	-	0.26	-	0.30	-	16	-	<p><u>Подготовка к текущему контролю:</u> Повторение материала по разделу "Общие вопросы информационной безопасности"</p>
1.1	Введение и основные понятия	9.78		1	-	0.5	-	0.13	-	0.15	-	8	-	
1.2	Комплексный подход к защите информации	9.78		0.5	-	1	-	0.13	-	0.15	-	8	-	
2	Методы защиты от несанкционированного доступа к информации в компьютерных системах	35.63		2.0	-	2.8	-	0.53	-	0.30	-	30	-	<p><u>Подготовка к текущему контролю:</u> Повторение материала по разделу "Информационная защита персонального компьютера (ПК)" <u>Изучение материалов литературных источников:</u> [1], п.3-4 [3], п.3</p>
2.1	Организация регистрационных баз данных	8.33		0.5	-	0.6	-	0.13	-	0.1	-	7	-	
2.2	Аутентификация при локальном доступе	9.54		0.5	-	0.8	-	0.14	-	0.1	-	8	-	
2.3	Аутентификация при локальном и удаленном доступе	9.28		0.5	-	0.6	-	0.13	-	0.05	-	8	-	
2.4	Аутентификация при удаленном доступе	8.48		0.5	-	0.8	-	0.13	-	0.05	-	7	-	
3	Программно-аппаратные средства защиты от несанкционированног	18.86		1.0	-	1.3	-	0.26	-	0.30	-	16	-	

	о доступа к информации в компьютерных системах												<u>Изучение материалов литературных источников:</u> [2], п.5
3.1	Разграничение прав пользователей компьютерных систем	10.58	0.5	-	0.8	-	0.13	-	0.15	-	9	-	
3.2	Средства защиты информации в операционных системах	8.28	0.5	-	0.5	-	0.13	-	0.15	-	7	-	
4	Криптографические методы и средства защиты информации	38.24	2.0	-	3.4	-	0.54	-	0.30	-	32	-	<u>Подготовка к текущему контролю:</u> Повторение материала по разделу "Введение в криптографию"
4.1	Введение в криптографию	9.50	0.5	-	0.8	-	0.15	-	0.05	-	8	-	<u>Изучение материалов литературных источников:</u>
4.2	Симметричная криптография	9.58	0.5	-	0.9	-	0.13	-	0.05	-	8	-	[3], п.7
4.3	Симметричная и асимметричная криптография	9.63	0.5	-	0.9	-	0.13	-	0.1	-	8	-	
4.4	Асимметричная криптография и ее применение	9.53	0.5	-	0.8	-	0.13	-	0.1	-	8	-	
5	Защита от вредоносных программ и несанкционированного копирования информационных ресурсов	31.71	1.5	-	3	-	0.41	-	0.3	-	26.5	-	<u>Подготовка к текущему контролю:</u> Повторение материала по разделу "Современные криптосистемы"
5.1	Криптография и стеганография	9.73	0.5	-	1	-	0.13	-	0.1	-	8	-	<u>Изучение материалов литературных источников:</u> [4], п.4
5.2	Защита от несанкционированного копирования	9.73	0.5	-	1	-	0.13	-	0.1	-	8	-	
5.3	Защита от вредоносных программ	12.25	0.5	-	1	-	0.15	-	0.1	-	10.5	-	

	Экзамен	36.0		-	-	-	-	-	-	-	0.3	-	35.7	
	Всего за семестр	180.00		8.0	-	12.0	-	2.00	-	1.50	0.3	120.5	35.7	
	Итого за семестр	180.00		8.0	-	12.0	2.00		1.50	0.3		156.2		

Примечание: Лек – лекции; Лаб – лабораторные работы; Пр – практические занятия; КПП – 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. Комплексный подход к обеспечению информационной безопасности

1.1. Введение и основные понятия

Проблема защиты информации и подходы к ее решению. Основные понятия защиты информации. Угрозы безопасности информации и каналы утечки информации.

1.2. Комплексный подход к защите информации

Классификация методов и средств защиты информации. Специфика программных средств. Правовое обеспечение защиты информации.

2. Методы защиты от несанкционированного доступа к информации в компьютерных системах

2.1. Организация регистрационных баз данных

Способы нарушения защищенности информации и защиты от него в компьютерных системах. Организация базы учетных записей пользователей в ОС Unix. Организация базы учетных записей пользователей в ОС Windows.

2.2. Аутентификация при локальном доступе

Способы аутентификации пользователей. Аутентификация пользователей на основе паролей. Аутентификация пользователей на основе модели «рукопожатия».

2.3. Аутентификация при локальном и удаленном доступе

Программно-аппаратная защита от локального НСД. Аутентификация пользователей на основе их биометрических характеристик. Протоколы прямой аутентификации.

2.4. Аутентификация при удаленном доступе

Протоколы непрямой аутентификации. Протокол IPSec. Виртуальные частные сети.

3. Программно-аппаратные средства защиты от несанкционированного доступа к информации в компьютерных системах

3.1. Разграничение прав пользователей компьютерных систем

Разграничение прав пользователей в ОС Windows. Дискреционное, мандатное и ролевое разграничение доступа к объектам.

3.2. Средства защиты информации в операционных системах

Подсистема безопасности ОС Windows. Разграничение доступа к объектам в ОС Windows. Разграничение прав пользователей в ОС Unix.

4. Криптографические методы и средства защиты информации

4.1. Введение в криптографию

Стандарты оценки безопасности компьютерных систем и информационных технологий. Элементы теории чисел. Способы симметричного шифрования.

4.2. Симметричная криптография

Абсолютно стойкий шифр. Генерация, хранение и распространение ключей. Криптографическая система DES и ее модификации. Криптографическая система ГОСТ 28147-89.

4.3. Симметричная и асимметричная криптография

Применение и обзор современных симметричных криптосистем. Принципы построения, свойства и применение асимметричных криптосистем. Криптографическая система RSA.

4.4. Асимметричная криптография и ее применение

Криптографические системы Диффи-Хеллмана, Эль-Гамала и эллиптических кривых. Электронная цифровая подпись и ее применение. Функции хеширования. Протокол SSL.

5. Защита от вредоносных программ и несанкционированного копирования информационных ресурсов

5.1. Криптография и стеганография

Криптографический интерфейс приложений ОС Windows. Файловая система с шифрованием в ОС Windows. Компьютерная стеганография и ее применение.

5.2. Защита от несанкционированного копирования

Принципы построения систем защиты от копирования. Защита инсталляционных дисков и установленного программного обеспечения. Защита программных средств от изучения.

5.3. Защита от вредоносных программ

Вредоносные программы, их признаки и классификация. Программные закладки и защита от них. Методы обнаружения и удаления вредоносных программ.

3.3. Темы практических занятий

1. Обеспечение информационной безопасности;
2. Несанкционированный доступ к информации в компьютерных системах;
3. Программно-аппаратные средства защиты;
4. Криптографические методы защиты информации;
5. Защита от вредоносных программ.

3.4. Темы лабораторных работ

не предусмотрено

3.5 Консультации

Групповые консультации по разделам дисциплины (ГК)

1. Обсуждение материалов по кейсам раздела "Общие вопросы информационной безопасности"
2. Обсуждение материалов по кейсам раздела "Информационная защита персонального компьютера (ПК)"
3. Обсуждение материалов по кейсам раздела "Направления обеспечения информационной безопасности"
4. Обсуждение материалов по кейсам раздела "Введение в криптографию"
5. Обсуждение материалов по кейсам раздела "Современные криптосистемы"

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	5	
Знать:							
методы разграничения полномочий пользователей и управления доступом к ресурсам в компьютерных системах и сетях	ПК-3(Компетенция)	+					Тестирование/Понятие информационной безопасности
способы построения симметричных и асимметричных криптографических систем	ПК-3(Компетенция)					+	Тестирование/Вредоносные программы
Уметь:							
применять методы разграничения полномочий пользователей и управления доступом к данным в компьютерных системах и сетях	ПК-3(Компетенция)			+			Лабораторная работа/Изучение программных средств защиты от несанкционированного доступа и разграничения прав пользователей
анализировать, выбирать и применять методы и средства защиты от вредоносных программ	ПК-3(Компетенция)				+		Лабораторная работа/Изучение программных средств шифрования, компьютерной стеганографии и защиты от вредоносных программ
использовать методы и средства криптографической защиты информации	ПК-3(Компетенция)		+				Лабораторная работа/Разработка программы разграничения полномочий пользователей на основе парольной аутентификации

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

4.1. Текущий контроль успеваемости

6 семестр

Форма реализации: Компьютерное задание

1. Вредоносные программы (Тестирование)
2. Понятие информационной безопасности (Тестирование)

Форма реализации: Письменная работа

1. Изучение программных средств защиты от несанкционированного доступа и разграничения прав пользователей (Лабораторная работа)
2. Изучение программных средств шифрования, компьютерной стеганографии и защиты от вредоносных программ (Лабораторная работа)
3. Разработка программы разграничения полномочий пользователей на основе парольной аутентификации (Лабораторная работа)

Балльно-рейтинговая структура дисциплины является приложением А.

4.2 Промежуточная аттестация по дисциплине

Экзамен (Семестр №6)

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

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

5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1 Печатные и электронные издания:

1. Зайцев А. П., Мещеряков Р. В., Шелупанов А. А.- "Технические средства и методы защиты информации", (7-е изд., испр.), Издательство: "Горячая линия-Телеком", Москва, 2018 - (442 с.)

<https://e.lanbook.com/book/111057>;

2. Малюк, А. А. Введение в защиту информации в автоматизированных системах : учебное пособие по специальностям, не входящим в группу специальностей в области информационной безопасности / А. А. Малюк, С. В. Пазизин, Н. С. Погожин . – 3-е изд., стереотип . – М. : Горячая Линия-Телеком, 2005 . – 147 с. - ISBN 5-935170-62-0 .;

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. 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 ..

5.2 Лицензионное и свободно распространяемое программное обеспечение:

1. СДО "Прометей";
2. Office;

3. Windows;
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. Электронная библиотека МЭИ (ЭБ МЭИ) - <http://elib.mpei.ru/login.php>
5. Портал открытых данных Российской Федерации - <https://data.gov.ru>
6. База открытых данных Министерства труда и социальной защиты РФ - <https://rosmintrud.ru/opendata>
7. База открытых данных профессиональных стандартов Министерства труда и социальной защиты РФ - <http://profstandart.rosmintrud.ru/obshchiy-informatsionnyy-blok/natsionalnyy-reestr-professionalnykh-standartov/>
8. База открытых данных Министерства экономического развития РФ - <http://www.economy.gov.ru>
9. База открытых данных Росфинмониторинга - <http://www.fedsfm.ru/opendata>
10. Электронная открытая база данных "Polpred.com Обзор СМИ" - <https://www.polpred.com>

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Тип помещения	Номер аудитории, наименование	Оснащение
Учебные аудитории для проведения лекционных занятий и текущего контроля	Ж-417/6, Белая мультимедийная студия	стол компьютерный, доска интерактивная, компьютерная сеть с выходом в Интернет, мультимедийный проектор, компьютер персональный
	Ж-417/7, Световая черная студия	стул, компьютерная сеть с выходом в Интернет, микрофон, мультимедийный проектор, экран, оборудование специализированное, компьютер персональный
Учебные аудитории для проведения практических занятий, КР и КП	Ж-417/1, Компьютерный класс ИДДО	стол преподавателя, стол компьютерный, шкаф для документов, шкаф для одежды, стол письменный, компьютерная сеть с выходом в Интернет, доска маркерная передвижная, компьютер персональный, принтер, кондиционер, стенд информационный
Учебные аудитории для проведения промежуточной аттестации	Ж-417/1, Компьютерный класс ИДДО	стол преподавателя, стол компьютерный, шкаф для документов, шкаф для одежды, стол письменный, компьютерная сеть с выходом в Интернет, доска маркерная передвижная, компьютер персональный, принтер, кондиционер, стенд информационный
Помещения для самостоятельной работы	НТБ-303, Компьютерный читальный зал	стол компьютерный, стул, стол письменный, вешалка для одежды, компьютерная сеть с выходом в Интернет, компьютер персональный, принтер, кондиционер
Помещения для	Ж-2006,	стол, стул, компьютер персональный,

консультирования	Конференц-зал ИДДО	кондиционер
Помещения для хранения оборудования и учебного инвентаря	Ж-417 /2а, Помещение для инвентаря	стеллаж для хранения инвентаря, экран, указка, архивные документы, дипломные и курсовые работы студентов, канцелярский принадлежности, спортивный инвентарь, хозяйственный инвентарь, запасные комплектующие для оборудования

БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА ДИСЦИПЛИНЫ

Методы и средства защиты информации

(название дисциплины)

6 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:

- КМ-1 Понятие информационной безопасности (Тестирование)
- КМ-2 Разработка программы разграничения полномочий пользователей на основе парольной аутентификации (Лабораторная работа)
- КМ-3 Изучение программных средств защиты от несанкционированного доступа и разграничения прав пользователей (Лабораторная работа)
- КМ-4 Изучение программных средств шифрования, компьютерной стеганографии и защиты от вредоносных программ (Лабораторная работа)
- КМ-5 Вредоносные программы (Тестирование)

Вид промежуточной аттестации – Экзамен.

Номер раздела	Раздел дисциплины	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4	КМ-5
		Неделя КМ:	3	6	8	11	14
1	Комплексный подход к обеспечению информационной безопасности						
1.1	Введение и основные понятия		+				
1.2	Комплексный подход к защите информации		+				
2	Методы защиты от несанкционированного доступа к информации в компьютерных системах						
2.1	Организация регистрационных баз данных			+			
2.2	Аутентификация при локальном доступе			+			
2.3	Аутентификация при локальном и удаленном доступе			+			
2.4	Аутентификация при удаленном доступе			+			
3	Программно-аппаратные средства защиты от несанкционированного доступа к информации в компьютерных системах						
3.1	Разграничение прав пользователей компьютерных систем				+		
3.2	Средства защиты информации в операционных системах				+		
4	Криптографические методы и средства защиты информации						

4.1	Введение в криптографию				+	
4.2	Симметричная криптография				+	
4.3	Симметричная и асимметричная криптография				+	
4.4	Асимметричная криптография и ее применение				+	
5	Защита от вредоносных программ и несанкционированного копирования информационных ресурсов					
5.1	Криптография и стеганография					+
5.2	Защита от несанкционированного копирования					+
5.3	Защита от вредоносных программ					+
Вес КМ, %:		20	20	20	20	20