Министерство науки и высшего образования РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Национальный исследовательский университет «МЭИ»

Направление подготовки/специальность: 09.04.01 Информатика и вычислительная техника

Наименование образовательной программы: Информационные и вычислительные технологии

Уровень образования: высшее образование - магистратура

Форма обучения: Очная

Рабочая программа дисциплины
КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Блок:	**Блок 1 «Дисциплины (модули)»**
Часть образовательной программы:	**Часть, формируемая участниками образовательных отношений**
№ дисциплины по учебному плану:	**Б4.Ч.02**
Трудоемкость в зачетных единицах:	**3 семестр - 2;**
Часов (всего) по учебному плану:	**72 часа**
Лекции	**3 семестр - 16 часов;**
Практические занятия	**3 семестр - 16 часов;**
Лабораторные работы	**не предусмотрено учебным планом**
Консультации	**проводится в рамках часов аудиторных занятий**
Самостоятельная работа	**3 семестр - 39,7 часа;**
в том числе на КП/КР	**не предусмотрено учебным планом**
Иная контактная работа	**проводится в рамках часов аудиторных занятий**
включая: **Контрольная работа**	
Промежуточная аттестация:	
Зачет	**3 семестр - 0,3 часа;**

Москва 2021

ПРОГРАММУ СОСТАВИЛ:

Преподаватель	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Андреева И.Н. Идентификатор: Rb5322c60-AndreevaIN-0472a135	И.Н. Андреева
(должность)	(подпись)	(расшифровка подписи)

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Андреева И.Н. Идентификатор: Rb5322c60-AndreevaIN-0472a135	И.Н. Андреева
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)
Заведующий выпускающей кафедры	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Топорков В.В. Идентификатор: Rc76a6458-ToporkovVV-1f71a135	В.В. Топорков
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель освоения дисциплины: изучение методов криптографической защиты информации

Задачи дисциплины

- изучение существующих решений по обеспечению информационной безопасности;
- освоение принципов построения и функционирования криптографических систем;
- приобретение навыков принятия эффективных решений при выборе средств для конкретного случая.

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-2 Способен применять методологии разработки программного обеспечения	ИД-1$_{ПК-2}$ Использует методы управления информационными ресурсами и создания информационных систем	знать: - методологию разработки системного и прикладного программного обеспечения для защиты данных. уметь: - работать с информационными ресурсами и системами для решения задач обеспечения информационной безопасности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к факультативным дисциплинам основной профессиональной образовательной программе Информационные и вычислительные технологии (далее – ОПОП), направления подготовки 09.04.01 Информатика и вычислительная техника, 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 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	Основные правовые нормы и классификация средств защиты информации и программного обеспечения	18	3	6	-	-	-	-	-	-	-	12	-	***Подготовка к контрольной работе:*** Изучение документов по правовым нормам и базовым принципыам организации систем защиты данных ***Подготовка к практическим занятиям:*** Изучение документов по правовым нормам и базовым принципыам организации систем защиты данных ***Изучение материалов литературных источников:*** [1], стр. 5-15 [2], стр. 6-9
1.1	Основные правовые нормы и классификация средств защиты информации и программного обеспечения	18		6	-	-	-	-	-	-	-	12	-	
2	Криптографические методы защиты. Электронные цифровые подписи	38		6	-	14	-	-	-	-	-	18	-	***Подготовка к контрольной работе:*** Изучение материалов по криптографическим методам защиты и электронным цифровым подписям ***Подготовка к практическим занятиям:*** Изучение материалов по криптографическим методам защиты и электронным цифровым подписям ***Изучение материалов литературных источников:*** [2], стр, 18-25 [3], стр. 40-44, 65-70 [5], стр. 48-58, 145-170
2.1	2.Криптографические методы защиты. Электронные цифровые подписи	38		6	-	14	-	-	-	-	-	18	-	
3	Стеганографические	15.7		4	-	2	-	-	-	-	-	9.7	-	***Подготовка к практическим занятиям:***

	методы защиты информации													Изучение материалов по стеганографии ***<u>Изучение материалов литературных источников:</u>*** [4], стр.7-42 [5], стр. 202-224
3.1	Стеганографические методы защиты информации	15.7		4	-	2	-	-	-	-	-	9.7	-	
	Зачет	0.3		-	-	-	-	-	-	-	0.3	-	-	
	Всего за семестр	**72.0**		**16**	**-**	**16**	**-**	**-**	**-**	**-**	**0.3**	**39.7**	**-**	
	Итого за семестр	**72.0**		**16**	**-**	**16**	**-**		**-**		**0.3**	**39.7**		

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. Основные правовые нормы и классификация средств защиты информации и программного обеспечения

1.1. Основные правовые нормы и классификация средств защиты информации и программного обеспечения

Основополагающие документы в области информационной безопасности. Основные информационные ресурсы и системы в области информационной безопасности. Понятие надежной системы, основные принципы политики безопасности. Классы безопасности. Классификация и выбор оптимального набора программных, технических средств их конфигурации для задач защиты от несанкционированного доступа..

2. Криптографические методы защиты. Электронные цифровые подписи

2.1. 2.Криптографические методы защиты. Электронные цифровые подписи

Основы криптографии. Базовые алгоритмы шифрования: подстановки, перестановки, гаммирование, аналитическое преобразование. Блочное шифрование. Симметричные системы шифрования. Сети Файстеля. Отечественный и международный стандарты симметричного шифрования. Асимметричные системы шифрования. Алгоритмы хеширования информации. Формирование и верификация цифровых подписей.

3. Стеганографические методы защиты информации

3.1. Стеганографические методы защиты информации

Классификация стеганографии. Классическая стеганогрфия и другие стеганографические методы. Стеганографические модели. Компьютерная и цифровая стеганография. Алгоритмы: метод LSB, эхо-методы, фазовое кодирование, метод расширенного спектра. Атаки на стегосистемы. Стеганография и цифровые водяные знаки..

3.3. Темы практических занятий

1. 1. Симметричные системы шифрования;
2. 2. Асимметричные системы шифрования;
3. 3. Принципы формирования электронных цифровых подписей;
4. 4. Стеганографические алгоритмы защиты данных.

3.4. Темы лабораторных работ

не предусмотрено

3.5 Консультации

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:					
методологию разработки системного и прикладного программного обеспечения для защиты данных	ИД-1$_{ПК-2}$		+	+	Контрольная работа/Алгоритмы симметричного шифрования Контрольная работа/Хеширование и ЭЦП
Уметь:					
работать с информационными ресурсами и системами для решения задач обеспечения информационной безопасности	ИД-1$_{ПК-2}$	+			Контрольная работа/Нормативные документы

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: Билеты (письменный опрос)

1. Алгоритмы симметричного шифрования (Контрольная работа)
2. Нормативные документы (Контрольная работа)
3. Хеширование и ЭЦП (Контрольная работа)

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» по совокупности результатов текущего контроля успеваемости.

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

5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1 Печатные и электронные издания:

1. Мельников, В. П. Информационная безопасность и защита информации : учебное пособие для вузов по специальности 230201 "Информационные системы и технологии" / В. П. Мельников, С. А. Клейменов, А. М. Петраков . – 3-е изд., стер . – М. : АКАДЕМИЯ, 2008 . – 336 с. – (Высшее профессиональное образование) . - ISBN 978-5-7695-4884-0 .;
2. Губонин, Н. С. Защита информации в системах передачи и обработки данных. Часть 1 : учебное пособие по курсу "Защита информации в системах передачи и обработки данных" по направлению "Радиотехника" / Н. С. Губонин, Нац. исслед. ун-т "МЭИ" . – М. : Изд-во МЭИ, 2013 . – 88 с. - ISBN 978-5-9902974-2-5 . http://elib.mpei.ru/action.php?kt_path_info=ktcore.SecViewPlugin.actions.document&fDocumentId=5673;
3. Губонин, Н. С. Ассиметричные криптосистемы и борьба с сетевыми угрозами : учебное пособие по курсу "Защита информации в системах передачи и обработки данных" по направлениям "Радиотехника", "Радиоэлектронные системы и комплексы" / Н. С. Губонин, Нац. исслед. ун-т "МЭИ" . – М. : Изд-во МЭИ, 2015 . – 84 с. - ISBN 978-5-7046-1666-5 . http://elib.mpei.ru/action.php?kt_path_info=ktcore.SecViewPlugin.actions.document&fDocumentId=7494;
4. Стеганография, цифровые водяные знаки и стеганоанализ / А. В. Аграновский, [и др.] . – М. : Вузовская книга, 2009 . – 220 с. - ISBN 978-5-9502-0401-2 .;
5. Рябко Б. Я., Фионов А. Н.- "Основы современной криптографии и стеганографии", (2-е изд.), Издательство: "Горячая линия-Телеком", Москва, 2016 - (232 с.) https://e.lanbook.com/book/111098.

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. **База данных ВИНИТИ online** - http://www.viniti.ru/
5. **База данных Web of Science** - http://webofscience.com/
6. **База данных Scopus** - http://www.scopus.com
7. **Национальная электронная библиотека** - https://rusneb.ru/
8. **ЭБС "Консультант студента"** - http://www.studentlibrary.ru/
9. **Электронная библиотека МЭИ (ЭБ МЭИ)** - http://elib.mpei.ru/login.php
10. **Портал открытых данных Российской Федерации** - https://data.gov.ru
11. **База открытых данных Министерства труда и социальной защиты РФ** - https://rosmintrud.ru/opendata
12. **База открытых данных профессиональных стандартов Министерства труда и социальной защиты РФ** - http://profstandart.rosmintrud.ru/obshchiy-informatsionnyy-blok/natsionalnyy-reestr-professionalnykh-standartov/
13. **База открытых данных Министерства экономического развития РФ** - http://www.economy.gov.ru
14. **База открытых данных Росфинмониторинга** - http://www.fedsfm.ru/opendata
15. **Электронная открытая база данных "Polpred.com Обзор СМИ"** - https://www.polpred.com
16. **Информационно-справочная система «Кодекс/Техэксперт»** - Http:\\proinfosoft.ru; http://docs.cntd.ru/

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Тип помещения	Номер аудитории, наименование	Оснащение
Учебные аудитории для проведения лекционных занятий и текущего контроля	Е-419, Учебная аудитория каф. "ВТ"	парта, стол преподавателя, стул, шкаф для документов, шкаф для одежды, компьютерная сеть с выходом в Интернет, мультимедийный проектор, доска маркерная передвижная, ноутбук
	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
Учебные аудитории для проведения практических занятий, КР и КП	Е-419, Учебная аудитория каф. "ВТ"	парта, стол преподавателя, стул, шкаф для документов, шкаф для одежды, компьютерная сеть с выходом в Интернет, мультимедийный проектор, доска маркерная передвижная, ноутбук
	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
Учебные аудитории для проведения промежуточной аттестации	Е-419, Учебная аудитория каф. "ВТ"	парта, стол преподавателя, стул, шкаф для документов, шкаф для одежды, компьютерная сеть с выходом в Интернет, мультимедийный проектор, доска маркерная передвижная, ноутбук
	Ж-120, Машинный	сервер, кондиционер

	зал ИВЦ	
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 консультирования	Е-411, Лаборатория каф. "ВТ"	стол, стол компьютерный, стул, шкаф для документов, шкаф для одежды, тумба, компьютерная сеть с выходом в Интернет, компьютер персональный
Помещения для хранения оборудования и учебного инвентаря	Е-403, Склад	стол для работы с документами, шкаф, шкаф для документов

Приложение А

БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА ДИСЦИПЛИНЫ

Криптографические методы защиты информации

(название дисциплины)

3 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:
КМ-1 Нормативные документы (Контрольная работа)
КМ-2 Алгоритмы симметричного шифрования (Контрольная работа)
КМ-3 Хеширование и ЭЦП (Контрольная работа)

Вид промежуточной аттестации – Зачет.

Номер раздела	Раздел дисциплины	Индекс КМ:	КМ-1	КМ-2	КМ-3
		Неделя КМ:	4	8	15
1	Основные правовые нормы и классификация средств защиты информации и про-граммного обеспечения				
1.1	Основные правовые нормы и классификация средств защиты информации и программного обеспечения		+		
2	Криптографические методы защиты. Электронные цифровые подписи				
2.1	2.Криптографические методы защиты. Электронные цифровые подписи			+	+
3	Стеганографические методы защиты информации				
3.1	Стеганографические методы защиты информации			+	+
Вес КМ, %:			20	40	40