

**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: Системы автоматизированного проектирования

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очная

**Рабочая программа дисциплины**  
**ЗАЩИТА ИНФОРМАЦИИ**

<b>Блок:</b>	<b>Блок 1 «Дисциплины (модули)»</b>
<b>Часть образовательной программы:</b>	<b>Обязательная</b>
<b>№ дисциплины по учебному плану:</b>	<b>Б1.О.27</b>
<b>Трудоемкость в зачетных единицах:</b>	<b>8 семестр - 4;</b>
<b>Часов (всего) по учебному плану:</b>	<b>144 часа</b>
<b>Лекции</b>	<b>8 семестр - 36 часа;</b>
<b>Практические занятия</b>	<b>не предусмотрено учебным планом</b>
<b>Лабораторные работы</b>	<b>8 семестр - 12 часов;</b>
<b>Консультации</b>	<b>8 семестр - 2 часа;</b>
<b>Самостоятельная работа</b>	<b>8 семестр - 93,5 часа;</b>
<b>в том числе на КП/КР</b>	<b>не предусмотрено учебным планом</b>
<b>Иная контактная работа</b>	<b>проводится в рамках часов аудиторных занятий</b>
<b>включая:</b> <b>Контрольная работа</b> <b>Лабораторная работа</b>	
<b>Промежуточная аттестация:</b>	
<b>Экзамен</b>	<b>8 семестр - 0,5 часа;</b>

**Москва 2019**

**ПРОГРАММУ СОСТАВИЛ:**

Преподаватель

(должность)

	<b>Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»</b>	
	<b>Сведения о владельце ЦЭП МЭИ</b>	
	Владелец	Андреева И.Н.
	Идентификатор	Rb5322c60-AndreevaIN-0472a135

(подпись)

И.Н. Андреева

(расшифровка  
подписи)

**СОГЛАСОВАНО:**

Руководитель  
образовательной программы

(должность, ученая степень, ученое звание)

	<b>Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»</b>	
	<b>Сведения о владельце ЦЭП МЭИ</b>	
	Владелец	Андреева И.Н.
	Идентификатор	Rb5322c60-AndreevaIN-0472a135

(подпись)

И.Н. Андреева

(расшифровка  
подписи)

Заведующий выпускающей  
кафедры

(должность, ученая степень, ученое звание)

	<b>Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»</b>	
	<b>Сведения о владельце ЦЭП МЭИ</b>	
	Владелец	Топорков В.В.
	Идентификатор	Rc76a6458-ToporkovVV-1f71a135

(подпись)

В.В. Топорков

(расшифровка  
подписи)

## 1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

**Цель освоения дисциплины:** Изучение методов, программных и технических средств защиты информации.

### Задачи дисциплины

- изучение существующих решений по обеспечению информационной безопасности;
- приобретение навыков принятия эффективных решений при выборе конфигурации и состава средств для конкретного случая;
- освоение принципов построения и функционирования криптографических систем;
- применение методик организации защиты корпоративных компьютерных сетей.

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-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ИД-2 <sub>оПК-3</sub> Применяет знания приемов безопасной работы в сети Интернет при поиске информации, связанной с профессиональной деятельностью	знать: - основные правовые нормы и базовые принципы организации систем защиты данных ПЭВМ и компьютерных сетей.
ПК-2 Способен определять конфигурацию и технические характеристики оборудования, необходимые для установки программного продукта	ИД-3 <sub>ПК-2</sub> Демонстрирует знание методов средств обеспечения защиты носителей информации, ЭВМ и компьютерных сетей от несанкционированного доступа	знать: - методику оптимального выбора программных, технических средств и их конфигурации для задач защиты от несанкционированного доступа.  уметь: - использовать приемы безопасной работы в сетях, включая поиск профильной информации в Интернет; - определять состав, устанавливать и работать с современными системами программирования для разработки средств защиты ПЭВМ и компьютерных сетей.

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к основной профессиональной образовательной программе Системы автоматизированного проектирования (далее – ОПОП), направления подготовки 09.03.01 Информатика и вычислительная техника, уровень образования: высшее образование - бакалавриат.

Требования к входным знаниям и умениям:

- знать современные инструментальные средства разработки приложений

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	Основные правовые нормы и классификация средств защиты информации и программного обеспечения от несанкционированного доступа	16	8	6	-	-	-	-	-	-	-	10	-	<p><b><u>Подготовка к контрольной работе:</u></b> Изучение документов по правовым нормам и базовым принципам организации систем защиты данных <b><u>Изучение материалов литературных источников:</u></b> [2], стр. 6-9 [3], стр. 5-15 [4], стр. 77-90</p>	
1.1	Основополагающие документы по информационной безопасности	16		6	-	-	-	-	-	-	-	10	-		
2	Идентификация и установление подлинности пользователей, устройств, вычислительных систем	34		10	4	-	-	-	-	-	-	-	20	-	<p><b><u>Подготовка к лабораторной работе:</u></b> Изучение материала по технологиям определения идентифицирующих параметров <b><u>Изучение материалов литературных источников:</u></b> [1], стр. 26-33 [3], стр. 26-35 [4], стр. 148-165</p>
2.1	Идентификация и аутентификация субъектов и объектов	34		10	4	-	-	-	-	-	-	-	20	-	
3	Криптографические методы защиты	29		10	4	-	-	-	-	-	-	-	15	-	
3.1	Системы шифрования	29	10	4	-	-	-	-	-	-	-	15	-	<p><b><u>Подготовка к лабораторной работе:</u></b> Изучение алгоритмов симметричного шифрования и вариантов их реализации специализированными функциями <b><u>Изучение материалов литературных источников:</u></b></p>	

													<b><u>источников:</u></b> [1], стр. 40-44, стр. 65-70 [2], стр. 8-25 [4], стр. 100-140
4	Методы и средства защиты компьютерных сетей	29	10	4	-	-	-	-	-	-	15	-	<b><u>Подготовка к лабораторной работе:</u></b> Изучение алгоритмов асимметричного шифрования и ЭЦП
4.1	Функции и сервисы безопасности сетей	29	10	4	-	-	-	-	-	-	15	-	<b><u>Изучение материалов литературных источников:</u></b> [1], стр. 45-49, стр. 60-64 [4], стр. 193-230
	Экзамен	36.0	-	-	-	-	2	-	-	0.5	-	33.5	
	<b>Всего за семестр</b>	<b>144.0</b>	<b>36</b>	<b>12</b>	<b>-</b>	<b>-</b>	<b>2</b>	<b>-</b>	<b>-</b>	<b>0.5</b>	<b>60</b>	<b>33.5</b>	
	<b>Итого за семестр</b>	<b>144.0</b>	<b>36</b>	<b>12</b>	<b>-</b>	<b>2</b>	<b>-</b>	<b>-</b>	<b>0.5</b>	<b>60</b>	<b>93.5</b>		

**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. Основные правовые нормы и классификация средств защиты информации и программного обеспечения от несанкционированного доступа

##### 1.1. основополагающие документы по 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. Идентификация и установление подлинности пользователей, устройств, вычислительных систем

##### 2.1. Идентификация и аутентификация субъектов и объектов

Идентификация и установление подлинности. Установление подлинности пользователя, файла, вычислительной системы. Выбор пароля. Установление полномочий. Матрица установления полномочий. Иерархические системы установления полномочий. Системы регистрации пользователей, событий, используемых ресурсов. Привязка программных средств к конкретному компьютеру. Критерии выбора системы защиты. Технические устройства защиты информации и программного обеспечения. Принципы действия электронных ключей.

#### 3. Криптографические методы защиты

##### 3.1. Системы шифрования

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..

#### 4. Методы и средства защиты компьютерных сетей

##### 4.1. Функции и сервисы безопасности сетей

Особенности защиты информации в компьютерных сетях. Алгоритмы хеширования информации. Формирование и верификация цифровых подписей. Функции и сервисы безопасности сетей. Межсетевые экраны: виды, принципы организации. Использование VPN-технологии для создания защищенных каналов передачи информации. Системы контроля содержания..

### **3.3. Темы практических занятий** не предусмотрено

### **3.4. Темы лабораторных работ**

1. 1. Защита приложений от несанкционированного использования;
2. 2. Изучение методов защиты программного обеспечения на основе криптографических алгоритмов;
3. 3. Изучение алгоритмов асимметричного шифрования и ЭЦП.

### **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	4	
<b>Знать:</b>						
основные правовые нормы и базовые принципы организации систем защиты данных ПЭВМ и компьютерных сетей	ИД-2опк-3	+				Контрольная работа/Нормативные документы
методику оптимального выбора программных, технических средств и их конфигурации для задач защиты от не-санкционированного доступа	ИД-3пк-2		+			Лабораторная работа/Идентификация и аутентификация субъектов и объектов
<b>Уметь:</b>						
определять состав, устанавливать и работать с современными системами программирования для разработки средств защиты ПЭВМ и компьютерных сетей	ИД-3пк-2				+	Лабораторная работа/Изучение алгоритмов асимметричного шифрования и ЭЦП
использовать приемы безопасной работы в сетях, включая поиск профильной информации в Интернет	ИД-3пк-2			+		Лабораторная работа/Защиты ПО с использованием криптографических алгоритмов

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

##### **4.1. Текущий контроль успеваемости**

**8 семестр**

Форма реализации: Билеты (письменный опрос)

1. Нормативные документы (Контрольная работа)

Форма реализации: Компьютерное задание

1. Защиты ПО с использованием криптографических алгоритмов (Лабораторная работа)
2. Идентификация и аутентификация субъектов и объектов (Лабораторная работа)
3. Изучение алгоритмов асимметричного шифрования и ЭЦП (Лабораторная работа)

Балльно-рейтинговая структура дисциплины является приложением А.

##### **4.2 Промежуточная аттестация по дисциплине**

*Экзамен (Семестр №8)*

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. 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](http://elib.mpei.ru/action.php?kt_path_info=ktcore.SecViewPlugin.actions.document&fDocumentId=7494);
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](http://elib.mpei.ru/action.php?kt_path_info=ktcore.SecViewPlugin.actions.document&fDocumentId=5673);
3. 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 .;
4. Шаньгин В. Ф.- "Информационная безопасность", Издательство: "ДМК Пресс", Москва, 2014 - (702 с.)  
[http://e.lanbook.com/books/element.php?pl1\\_id=50578](http://e.lanbook.com/books/element.php?pl1_id=50578).

##### **5.2 Лицензионное и свободно распространяемое программное обеспечение:**

1. СДО "Прометей";
2. Office;

3. Windows;
4. Майнд Видеоконференции;
5. Visual Studio.

### **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](http://biblioclub.ru/index.php?page=main_ub_red)
3. Научная электронная библиотека - <https://elibrary.ru/>
4. База данных ВИНТИ online - <http://www.viniti.ru/>
5. База данных журналов издательства Elsevier - <https://www.sciencedirect.com/>
6. Электронные ресурсы издательства Springer - <https://link.springer.com/>
7. База данных Web of Science - <http://webofscience.com/>
8. База данных Scopus - <http://www.scopus.com>
9. Национальная электронная библиотека - <https://rusneb.ru/>
10. ЭБС "Консультант студента" - <http://www.studentlibrary.ru/>
11. База данных Association for Computing Machinery Digital Library - <https://dl.acm.org/about/content>
12. База данных IEL издательства IEEE (Institute of Electrical and Electronics Engineers, Inc.) - <https://ieeexplore.ieee.org/Xplore/home.jsp?reload=true>
13. База данных Computers & Applied Sciences Complete (CASC) - <http://search.ebscohost.com>
14. Журнал Science - <https://www.sciencemag.org/>
15. Электронная библиотека МЭИ (ЭБ МЭИ) - <http://elib.mpei.ru/login.php>
16. Портал открытых данных Российской Федерации - <https://data.gov.ru>
17. База открытых данных Министерства труда и социальной защиты РФ - <https://rosmintrud.ru/opendata>
18. База открытых данных профессиональных стандартов Министерства труда и социальной защиты РФ - <http://profstandart.rosmintrud.ru/obshchiy-informatsionnyy-blok/natsionalnyy-reestr-professionalnykh-standartov/>
19. База открытых данных Министерства экономического развития РФ - <http://www.economy.gov.ru>
20. База открытых данных Росфинмониторинга - <http://www.fedsfm.ru/opendata>
21. Электронная открытая база данных "Polpred.com Обзор СМИ" - <https://www.polpred.com>
22. 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-405, Учебная аудитория каф. "ВТ"	парта, стол преподавателя, стул, шкаф для документов, доска меловая, компьютерная сеть с выходом в Интернет, доска маркерная передвижная
	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
Учебные аудитории для проведения лабораторных занятий	Е-406/2, Учебная лаборатория каф. "ВТ"	парта, стол преподавателя, стол компьютерный, стул, шкаф для документов, компьютерная сеть с

		выходом в Интернет, сервер, компьютер персональный
	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
Учебные аудитории для проведения промежуточной аттестации	Е-405, Учебная аудитория каф. "ВТ"	парта, стол преподавателя, стул, шкаф для документов, доска меловая, компьютерная сеть с выходом в Интернет, доска маркерная передвижная
	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
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

## БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА ДИСЦИПЛИНЫ

## Защита информации

(название дисциплины)

## 8 семестр

**Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:**

- КМ-1 Нормативные документы (Контрольная работа)  
 КМ-2 Идентификация и аутентификация субъектов и объектов (Лабораторная работа)  
 КМ-3 Защиты ПО с использованием криптографических алгоритмов (Лабораторная работа)  
 КМ-4 Изучение алгоритмов асимметричного шифрования и ЭЦП (Лабораторная работа)

**Вид промежуточной аттестации – Экзамен.**

Номер раздела	Раздел дисциплины	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
		Неделя КМ:	3	5	9	13
1	Основные правовые нормы и классификация средств защиты информации и программного обеспечения от несанкционированного доступа					
1.1	Основополагающие документы по информационной безопасности		+			
2	Идентификация и установление подлинности пользователей, устройств, вычислительных систем					
2.1	Идентификация и аутентификация субъектов и объектов			+		
3	Криптографические методы защиты					
3.1	Системы шифрования				+	
4	Методы и средства защиты компьютерных сетей					
4.1	Функции и сервисы безопасности сетей					+
Вес КМ, %:			15	30	30	25