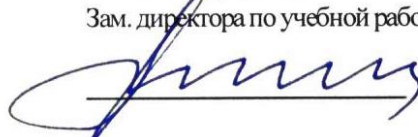


**Космический факультет**  
Кафедра «Прикладная математика, информатика и вычислительная техника» (КЗ)

«УТВЕРЖДАЮ»

Зам. директора по учебной работе МФ, д.т.н.

 Макуев В.А.

« 29 » 04 2019 г.

## РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ «ЗАЩИТА ИНФОРМАЦИИ»

Направление подготовки

**09.03.01 «Информатика и вычислительная техника»**

Направленность подготовки

**Вычислительные машины, комплексы, системы и сети**

Квалификация выпускника

**бакалавр**

Форма обучения – очная

Срок освоения – 4 года

Курс – IV

Семестр – 8

Трудоемкость дисциплины:	– <u>4</u> зачетных единиц
Всего часов	– <u>144</u> час.
Из них:	
Аудиторная работа	– <u>60</u> час.
Из них:	
лекций	– <u>40</u> час.
лабораторных работ	– <u>20</u> час.
Самостоятельная работа	– <u>48</u> час.
Подготовка к экзамену	– <u>36</u> час.
Формы промежуточной аттестации:	
экзамен	– <u>8</u> семестр

Мытищи, 2019 г.

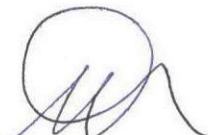
Рабочая программа составлена на основании ОПОП ВО, разработанной в соответствии с требованиями ФГОС ВО по данному направлению подготовки, направленностью подготовки, нормативными документами Министерства науки и высшего образования, университета и локальными актами филиала.

Автор:

Доцент кафедры прикладной математики, информатики и вычислительной техники, к.т.н., доцент

(должность, ученая степень, ученое звание)

(подпись)  
«19» 04 2019г.

  
А. М. Ветошкин

(Ф.И.О.)

Рецензент:

Доцент кафедры информационно-измерительных системы и технологий приборостроения, к.т.н., доцент

(должность, ученая степень, ученое звание)

(подпись)  
«19» 04 2019г.

  
П. А. Тарасенко

(Ф.И.О.)

Рабочая программа рассмотрена и одобрена на заседании кафедры «Прикладная математика, информатика и вычислительная техника» (КЗ МФ)

Протокол № 9 от «19» 04 2019г.

Заведующий кафедрой, д.ф.-м.н., профессор

(ученая степень, ученое звание)

(подпись)  


А. А. Малашин

(Ф.И.О.)

Рабочая программа одобрена на заседании научно-методического совета Космического факультета

Протокол № 6 от «26» 04 2019г.

Декан факультета, к.т.н., доцент

(ученая степень, ученое звание)

(подпись)  


Н. Г. Поярков

(Ф.И.О.)

Рабочая программа соответствует всем необходимым требованиям, электронный вариант со всеми приложениями передан в отдел образовательных программ МФ (ООП МФ)

Начальник ООП МФ, к.т.н., доцент

(ученая степень, ученое звание)

(подпись)  
«28» 04 2019г.

А.А. Шевляков

(Ф.И.О.)

## СОДЕРЖАНИЕ

ВЫПИСКА ИЗ ОПОП ВО .....	
1. ЦЕЛИ ОСВОЕНИЯ И ЗАДАЧИ ДИСЦИПЛИНЫ, ЕЕ МЕСТО В УЧЕБНОМ ПРОЦЕССЕ .....	
1.1. Цель освоения дисциплины .....	
1.2. Планируемые результаты обучения по дисциплине ( <i>модулю</i> ), соотнесенные с планируемыми результатами освоения образовательной программы .....	
1.3. Место дисциплины в структуре образовательной программы .....	
2. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ .....	
3. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ .....	
3.1. Тематический план .....	
3.2. Учебно-методическое обеспечение для контактной работы обучающихся с преподавателем .....	
3.2.1. Содержание разделов дисциплины, объем в лекционных часах .....	
3.2.2. Практические занятия <i>и(или) семинары</i> .....	
3.2.3. Лабораторные работы .....	
3.2.4. Контроль самостоятельной работы обучающихся .....	
3.2.5. Инновационные формы учебных занятий .....	
3.3. Учебно-методическое обеспечение для самостоятельной работы обучающихся по дисциплине .....	
3.3.1. Расчетно-графические <i>и(или) расчетно-проектировочные работы</i> .....	
3.3.2. Рефераты .....	
3.3.3. Контрольные работы .....	
3.3.4. Другие виды самостоятельной работ .....	
3.3.5. Курсовой проект <i>или курсовая работа</i> .....	
4. ТЕКУЩИЙ КОНТРОЛЬ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ .....	
4.1. Текущий контроль успеваемости обучающихся .....	
4.2. Промежуточная аттестация обучающихся .....	
5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ .....	
5.1. Рекомендуемая литература .....	
5.1.1. Основная и дополнительная литература .....	
5.1.2. Учебные и учебно-методические пособия для подготовки к контактной работе обучающихся с преподавателем и для самостоятельной работы обучающихся .....	
5.1.3. Нормативные документы .....	
5.1.4. Ресурсы информационно-телекоммуникационной сети «Интернет» и другие электронные информационные источники .....	
5.2. Информационные технологии и другие средства, используемые при осуществлении образовательного процесса по дисциплине .....	
5.3. Раздаточный материал .....	
6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА .....	
7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ .....	
8. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПРЕПОДАВАТЕЛЮ .....	
ПРИЛОЖЕНИЯ	
Карта обеспеченности литературой дисциплины .....	
Учебно-методические карты дисциплины .....	
Графики учебного процесса и самостоятельной работы обучающихся по дисциплине .....	
Протокол междисциплинарного согласования рабочей программы дисциплины . ( <i>при необходимости</i> )	
Протокол о временном разрешении использования литературы при изучении дисциплины .....	
.....( <i>при необходимости</i> )	
Протокол обновлений, дополнений и изменений в рабочей программе дисциплины .....	
.....( <i>при необходимости</i> )	
Фонд оценочных средств по дисциплине .....	

**Выписка из ООП ВПО** по направлению 09.03.01 «Информатика и вычислительная техника» для профиля(ей) подготовки Вычислительные машины, комплексы, системы и сети для учебной дисциплины «Защита информации»:

<b>Индекс</b>	<b>Наименование дисциплины и ее основные разделы (дидактические единицы)</b>	<b>Всего часов</b>
<b>Б1.О.12</b>	<b>Защита информации.</b> Криптография, стойкость шифров; абсолютно стойкий шифр, шифры подстановки; шифры перестановки, шифрование с открытым ключом, алгоритм шифрования RSA, теория чисел, группы, кольца, поля	<b>144</b>

# 1. ЦЕЛИ ОСВОЕНИЯ И ЗАДАЧИ ДИСЦИПЛИНЫ, ЕЕ МЕСТО В УЧЕБНОМ ПРОЦЕССЕ

## 1.1. Цель освоения дисциплины

Основная цель преподавания курса «защита информации» состоит в получении студентами знаний по основам защиты информации для обеспечения всесторонней технической подготовки будущего специалиста. В результате изучения курса студенты должны получить знания для обеспечения всесторонней технической подготовки будущего специалиста в области касающейся защиты информации и сохранении частных данных..

## 1.2. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

В результате освоения дисциплины обучающийся готовится к решению задач профессиональной деятельности следующих типов:

### *Проектная деятельность:*

Выполнение работ по созданию и модификации аппаратных и программно-аппаратных компонентов ИТ-систем.

В соответствии с ОПОП ВО по данному направлению и направленности подготовки процесс обучения по данной дисциплине направлен на формирование следующих планируемых результатов освоения образовательной программы (компетенций обучающихся и их индикаторов), установленных образовательной программой:

Код и наименование компетенции (результата освоения образовательной программы)	Код и наименование индикатора достижения компетенции
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;	ОПК-3.1. Знает приемы и методы решения стандартных задач профессиональной деятельности, основные правила обеспечения информационной безопасности
	ОПК-3.2. Умеет решать стандартные задачи профессиональной деятельности на основе математической, информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
	ОПК-3.3. Владеет методиками решения стандартных задач профессиональной деятельности на основе математической, информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
ОПК-9. Способен осваивать методики использования программных средств для решения практических задач.	ОПК-9.1. Знает подходы к использованию программных средств для решения практических задач
	ОПК-9.2. Умеет осваивать отечественные и зарубежные методики использования программных средств для решения практических задач
	ОПК-9.3. Владеет практическими навыками применения современных инструментальных средств проектирования и отработки ИТ-систем

Перечень планируемых результатов обучения по дисциплине (ЗУНов), соотнесенных с установленными в образовательной программе индикаторами достижения компетенций:

Код и наименование индикатора достижения компетенции	Наименование показателя оценивания (результата обучения по дисциплине)
ОПК-3.1. Знает приемы и методы решения стандартных задач профессиональной деятельности, основные правила обеспечения информационной безопасности	Знать: – принципы построения архитектуры программного обеспечения и виды архитектур программного обеспечения; – основные правила обеспечения информационной безопасности
ОПК-3.2. Умеет решать стандартные задачи профессиональной деятельности на основе математической, информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Уметь: – применять методы и средства проектирования и реализации программного обеспечения;
ОПК-3.3. Владеет методиками решения стандартных задач профессиональной деятельности на основе математической, информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Владеть: – навыками решения стандартных задач профессиональной деятельности на основе математической, информационной и библиографической культуры с применением информационно-коммуникационных технологий
ОПК-9.1. Знает подходы к использованию программных средств для решения практических задач	Знать: – методы и средства проектирования программно-аппаратных компонентов ИТ-систем;
ОПК-9.2. Умеет осваивать отечественные и зарубежные методики использования программных средств для решения практических задач	Уметь: – проектировать новые и модифицировать существующие программно-аппаратные компоненты ИТ-систем;
ОПК-9.3. Владеет практическими навыками применения современных инструментальных средств проектирования и отработки ИТ-систем	Владеть: – практическими навыками применения современных инструментальных средств проектирования и отработки программно-аппаратных компонентов ИТ-систем.

### 1.3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Данная дисциплина входит в часть, формируемую участниками образовательных отношений Блока 1 «Дисциплины (модули)».

Изучение данной дисциплины базируется на знаниях, умениях и навыках, полученных при изучении: Программирование на языках высокого уровня.

Полученные при изучении данной дисциплины знания, умения и навыки будут использоваться при изучении следующих дисциплин: Системное программное

## 2. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Вид учебной работы	Часов		Семестры	
	всего	в том числе в инновацио нных формах	8	
<b>Общая трудоемкость дисциплины:</b>	<b>144</b>		<b>144</b>	
<b>Переаттестовано:</b> <i>(только при обучении по индивидуальным планам)</i>	-	-	-	-
<b>Контактная работа обучающихся с преподавателем:</b>	<b>60</b>	<b>14</b>	<b>60</b>	
Лекции (Л)	40		40	
Практические занятия (Пз) или семинары (С)				
Лабораторные работы (Лр)	20	14	20	
Контроль самостоятельной работы студентов (КСР)				
<b>Самостоятельная работа студента:</b>	<b>48</b>		<b>48</b>	
Проработка прослушанных лекций (Л), - 20	10	-	10	
Подготовка к лабораторным работам (Лр) – 10	20	-	20	
Подготовка к контрольным работам (Кр) - 2	6	-	6	
Проведение других видов самостоятельной работы (Др)	12	-	12	
<b>Подготовка к экзамену:</b> <i>(только при наличие экзамена(ов) – по 36 час на 1 экзамен)</i>	36		36	
<b>Вид промежуточного контроля:</b> <i>(зачет (Зач), экзамен (Э))</i>	Э	-	Э	

### 3. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

#### 3.1. ТЕМАТИЧЕСКИЙ ПЛАН

№ п/п	Разделы дисциплины	Индикаторы достижения компетенций	Аудиторные занятия			Самостоятельная работа обучающегося и формы ее контроля				Текущий контроль результатов обучения и промежуточная аттестация, баллов по модулям (мин./макс.)
			Л, часов	№ Пз (С)	№ Лр	№ РГР (Дз)	№ Р	№ Кр	Др часов	
<b>7 семестр</b>										
1.	Теория чисел	ОК-7, ОПК-1, ОПК-4	6		1,2			1,2	12	12/20
2.	Алгебра;	ОК-7, ОПК-1, ОПК-4	6		-					
3.	Криптография;	ОПК-4, ПК-1	10		-					
4.	Шифрование с открытым ключом	ОК-7, ОПК-1, ОПК-4, ПК-1	12		3-10					
5.	Целочисленная арифметика многократной точности;	ОПК-4, ПК-1	6		-					30/50
ИТОГО текущий контроль результатов обучения в 7 семестре										<b>42/70</b>
Промежуточная аттестация (экзамен)										<b>18/30</b>
<b>ИТОГО</b>										<b>60/100</b>

#### 3.2. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДЛЯ КОНТАКТНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ С ПРЕПОДАВАТЕЛЕМ

На контактную работу обучающихся с преподавателем, согласно учебному плану, отводится – 60 часов.

Контактная работа обучающихся с преподавателем *включает в себя:*

- лекции – 40 часов;
- лабораторные работы – 20 часов;

##### 3.2.1. СОДЕРЖАНИЕ РАЗДЕЛОВ ДИСЦИПЛИНЫ, ОБЪЕМ В ЛЕКЦИОННЫХ ЧАСАХ (Л) – 36 ЧАСОВ

№ Л	Раздел (модуль) дисциплины и его содержание	Объем, часов
1	<b>Теория чисел;</b> сравнения; НОД; алгоритм Евклида; непрерывная дробь; подходящие дроби	2
2	Нахождение обратной величины по модулю; функция Эйлера;	2
3	Теорема Эйлера; теорема Ферма; символ Лежандра	2
4	<b>Алгебра;</b> группа, порядок группы; подгруппа; циклическая группа; теорема Лагранжа.	2
5	Кольца; примеры колец; кольцо $Z_m$ , делители нуля.	2
6	Поля; примеры полей; поле Галуа $GF(q)$ ; мультипликативная группа поля Галуа;	2



<i>№ Л</i>	<i>Раздел (модуль) дисциплины и его содержание</i>	<i>Объем, часов</i>
	примитивный элемент, расширения полей, подполя, характеристика поля	
7	<b>Криптография</b> ; исторические примеры шифров;	2
8	Стойкость шифров; абсолютно стойкий шифр; проблема распространения ключей; шифр Цезаря;	2
9,10	Аффинное преобразование; биграммы; шифры подстановки; шифры перестановки;	3
10,11	Потоковые шифры; блочные шифры; симметрические шифросистемы; стандарты шифрования: DES, AES, ГОСТ-28147-89	3
12	<b>Шифрование с открытым ключом</b> ; односторонняя функция; функция с секретом; схема Диффи-Хеллмана;	2
13	Алгоритм шифрования RSA;	2
14	Задачи трудные для решения – вычисление дискретного логарифма, разложение на множители большого числа	2
15	Электронная подпись; протокол аутентификации; протокол подбрасывания монеты по телефону; электронное голосование; электронные торги;.	2
16	Схема Шамира; криптосистема Рабина; криптосистема Эль-Гамала	2
17	Эллиптические кривые; группы точек на эллиптических кривых; криптосистемы на эллиптических кривых	2
18,19	<b>Целочисленная арифметика многократной точности</b> ; расширенный двоичный НОД; сложение, вычитание, умножение, возведение в степень слева-направо и справа-налево;	3
19,20	Редукция Монтгомери, возведение в степень по Монтгомери	3

В таблицу вносятся номера лекций, номера и названия разделов (тем) дисциплины, их содержание с разбивкой на лекции и лекционные часы

### 3.2.2. ПРАКТИЧЕСКИЕ ЗАНЯТИЯ (ПЗ) или СЕМИНАРЫ (С) – 0 ЧАСОВ

ПРАКТИЧЕСКИЕ ЗАНЯТИЯ УЧЕБНЫМ ПЛАНОМ НЕ ПРЕДУСМОТРЕНЫ.

### 3.2.3. ЛАБОРАТОРНЫЕ РАБОТЫ (ЛР) – 20 ЧАСОВ

<i>№ Лр</i>	<i>Тема лабораторной работы</i>	<i>Объем часов</i>	<i>Раздел (модуль) дисциплины</i>	<i>Виды контроля текущей успеваемости</i>
1	Вычисление вычетов по модулю; Возведение в степень	2	1	Устный опрос
2	Нахождение обратной величины по модулю, примитивный корень	2	1	Устный опрос
3	Схема Диффи-Хеллмана. Часть 1.	2	4	Устный опрос
4	Схема Диффи-Хеллмана. Часть 2.	2	4	Устный опрос
5	Реализация схемы RSA. Часть 1.	2	4	Устный опрос
6	Реализация схемы RSA. Часть 2.	2	4	Устный опрос
7	Схема Шамира. Часть 1.	2	4	Устный опрос

<i>№ Лр</i>	<i>Тема лабораторной работы</i>	<i>Объем часов</i>	<i>Раздел (модуль) дисциплины</i>	<i>Виды контроля текущей успеваемости</i>
8	Схема Шамира. Часть 2.	2	4	Устный опрос
9	Криптосистема Эль-Гамала. Часть 1.	2	4	Устный опрос
10	Криптосистема Эль-Гамала. Часть 2.	2	4	Устный опрос

### **3.2.4. ИННОВАЦИОННЫЕ ФОРМЫ УЧЕБНЫХ ЗАНЯТИЙ**

При изучении данной дисциплины применяются следующие инновационные формы учебных занятий:

- Выступление студента в роли обучающего
- Работа в команде (группах)
- Самостоятельная работа обучающегося за компьютером

При этом предусматривается использование таких вспомогательных средств, как: Персональные ЭВМ с предустановленным инструментальным и справочным программным обеспечением

### **3.3. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ**

*На самостоятельную работу обучающихся, согласно учебному плану, отводится*

*– 48 часов.*

Самостоятельная работа студентов включает в себя:

1. Проработку прослушанных лекций, изучение учебного материала, перенесенного с аудиторных занятий на самостоятельную проработку – 10 часов
2. Подготовку к лабораторным работам. – 20 часов
3. Другие виды самостоятельной работы – 12 часов
4. Подготовку к контрольной работе – 6 часов

#### **3.3.1. РАСЧЕТНО-ГРАФИЧЕСКИЕ (РГР) ИЛИ РАСЧЕТНО-ПРОЕКТИРОВОЧНЫЕ (РПР) РАБОТЫ – 0 ЧАСОВ**

РАСЧЕТНО-ГРАФИЧЕСКИЕ РАБОТЫ УЧЕБНЫМ ПЛАНОМ НЕ ПРЕДУСМОТРЕНЫ.

#### **3.3.2. РЕФЕРАТЫ – 0 ЧАСОВ**

РЕФЕРАТЫ УЧЕБНЫМ ПЛАНОМ НЕ ПРЕДУСМОТРЕНЫ.

#### **3.3.3. КОНТРОЛЬНЫЕ РАБОТЫ (КР) – 6 ЧАСОВ**

*Выполняется(ются) \_\_ контрольная(ые) работа(ы) по следующим темам:*

<i>№ Кр</i>	<i>Тема контрольной работы</i>	<i>Объем часов</i>	<i>Раздел дисциплины</i>
1,2	<i>Вычисление обратной величины по модулю</i>	6	1

### 3.3.4. ДРУГИЕ ВИДЫ САМОСТОЯТЕЛЬНОЙ РАБОТЫ (ДР) – 12 ЧАСОВ

На другие виды самостоятельной работы отводится 12 часов.

### 3.3.5. КУРСОВОЙ ПРОЕКТ (КП) ИЛИ КУРСОВАЯ РАБОТА (КР) – 0 ЧАСОВ

Курсовой проект или курсовая работа учебным планом не предусмотрены

## 4. ТЕКУЩИЙ КОНТРОЛЬ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Распределение часов контактной работы обучающихся с преподавателем и самостоятельной работы обучающихся, сроки выдачи заданий, их выполнения и контроля текущей успеваемости обучающихся по всем видам запланированных работ, формы текущего контроля успеваемости и промежуточной аттестации обучающихся, а также формирование планируемых результатов освоения образовательной программы (компетенций обучающихся, установленных ФГОС ВО или их элементов) по неделям семестра представлены в учебно-методических картах дисциплины и графиках учебного процесса по ней, которые сформированы как отдельные документы, являются приложениями к рабочей программе и структурно входят в состав учебно-методического комплекса дисциплины.

Оценочные средства по всем заявленным в рабочей программе видам контактной работы обучающихся с преподавателем и самостоятельной работы обучающихся, формам контроля текущей успеваемости и промежуточной аттестации обучающихся, утвержденные критерии оценки по ним и методика начисления рейтинговых баллов, а также перечень планируемых результатов освоения образовательной программы (компетенций обучающихся, установленных ФГОС ВО или их элементов) и отнесенные к ним планируемые результаты обучения (знания, умения и навыки), представлены в Фонде оценочных средств по дисциплине, который сформирован как отдельный документ, является приложением к рабочей программе и структурно входит в состав учебно-методического комплекса дисциплины.

### 4.1. ТЕКУЩИЙ КОНТРОЛЬ УСПЕВАЕМОСТИ ОБУЧАЮЩИХСЯ

Для оценки текущей успеваемости используются следующие формы текущего контроля:

№ п/п	Раздел дисциплины	Форма текущего контроля	Формируемые компетенции	Текущий контроль результатов обучения, баллов (мин./макс.)
1	1	Защита лабораторной работы № 1	ОК-7, ОПК-1, ОПК-4	4/6
2	1	Защита лабораторной работы № 2	ОК-7, ОПК-1, ОПК-4, ПК-1	4/6
	1	Выполнение контрольной работы №1	ОК-7, ОПК-1, ОПК-4, ПК-1	4/8
		<b>Всего за модуль:</b>		<b>12/20</b>
3	4	Защита лабораторной работы № 3	ОК-7, ОПК-1, ОПК-4, ПК-1	3/5
4	4	Защита лабораторной работы № 4	ОК-7, ОПК-1, ОПК-4, ПК-1	3/5
5	4	Защита лабораторной работы № 5	ОК-7, ОПК-1, ОПК-4, ПК-1	3/5
6	4	Защита лабораторной работы № 6	ОК-7, ОПК-1, ОПК-4, ПК-1	3/5
7	4	Защита лабораторной работы № 7	ОК-7, ОПК-1, ОПК-4, ПК-1	3/5
8	4	Защита лабораторной работы № 8	ОК-7, ОПК-1, ОПК-4, ПК-1	3/5
9	4	Защита лабораторной работы № 9	ОК-7, ОПК-1, ОПК-4, ПК-1	3/5
10	4	Защита лабораторной работы № 10	ОК-7, ОПК-1, ОПК-4, ПК-1	3/5
11	1	Выполнение контрольной работы №2	ОК-7, ОПК-1, ОПК-4, ПК-1	6/10
		<b>Всего за модуль:</b>		<b>30/50</b>
			<b>Итого:</b>	<b>42/70</b>

Обучающиеся, не выполнившие в полном объеме установленных требований и не набравшие суммарное количество рейтинговых баллов по текущему контролю успеваемости выше минимально установленных, не допускаются к промежуточной аттестации по данной дисциплине, как не выполнившие график учебного процесса по данной дисциплине.

#### 4.2. ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ОБУЧАЮЩИХСЯ

Для оценки результатов изучения дисциплины используются следующие формы промежуточной аттестации:

Семестр	Разделы дисциплины	Форма промежуточного контроля	Проставляется ли оценка в приложение к диплому	Промежуточная аттестация, баллов (мин./макс.)
7	1 - 5	экзамен	да	18/30

Обучающийся, выполнивший все предусмотренные учебным планом задания и сдавший все контрольные мероприятия по текущему контролю результатов обучения и прошедший промежуточную аттестацию, получает итоговую оценку по дисциплине за семестр в соответствии со шкалой:

Рейтинг	Оценка на экзамене, дифференцированном зачете	Оценка на зачете
85 – 100	отлично	зачет
71 – 84	хорошо	зачет
60 – 70	удовлетворительно	зачет
0 – 59	неудовлетворительно	незачет

## 5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

### 5.1. РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

#### 5.1.1. ОСНОВНАЯ И ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА

Основная литература:

1. Куприянов А.И. Основы защиты информации : Учебное пособие для студ. вузов, обуч. по спец. "Радиоэлектрон. системы", "Средства радиоэлектрон. борьбы" и "Информац. системы и технологии" / А.В. Сахаров, В.А. Шевцов. - 2-е изд., стереотип. - М. : Академия, 2007. - 253 с. - (Высшее профессиональное образование).
2. Коблиц Н. Курс теории чисел и криптографии – Научное изд-во ТВП, 2016, 254с.
3. Грибунин В.Г. Комплексная система защиты информации на предприятии : Учебное пособие для студ. вузов, обуч. по спец. "Организация и технология защиты информации", "Комплексная защита объектов информатизации" направ.подгот. / В.В.Чудовский. - М. : Академия, 2009. - 411 с. - (Высшее профессиональное образование).

Дополнительная литература:

4. Казарин О.В. Методология защиты программного обеспечения : Монография / МГУ; под ред. В.А. Садовниченко, В.П. Шерстюка. - М. : МЦНМО, 2009. - 464 с.: ил. - (Научные проблемы безопасности и противодействия терроризму).
5. Меньшаков Ю.К. Защита объектов и информации от технических средств разведки : Учеб.пособие / Рос.гос.гуманитарный ун-т. - М. : РГГУ, 2002. - 398 с.
6. Фороузан Б.А. Криптография и безопасность сетей: Учебное пособие. – М.:БИНОМ, 2010. -784 с.

#### 5.1.2. УЧЕБНЫЕ И УЧЕБНО-МЕТОДИЧЕСКИЕ ПОСОБИЯ ДЛЯ ПОДГОТОВКИ К КОНТАКТНОЙ РАБОТЕ ОБУЧАЮЩИХСЯ С ПРЕПОДАВАТЕЛЕМ И ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

## ОБУЧАЮЩИХСЯ

Баранова Е.К. Криптографические методы защиты информации. Лабораторный практикум : учебное пособие. – М.: КНОРУС, 2015. – 200с.

### 5.1.3. НОРМАТИВНЫЕ ДОКУМЕНТЫ

7. ГОСТ 19.701-90 (ИСО 5807-85) Схемы алгоритмов, программ, данных и систем.
8. ГОСТ 19781-90 Обеспечение систем обработки информации программное. Термины и определения.

### 5.1.4. ИНТЕРНЕТ-РЕСУРСЫ И ДРУГИЕ ЭЛЕКТРОННЫЕ ИНФОРМАЦИОННЫЕ ИСТОЧНИКИ

1. <http://www.intuit.ru>
2. <http://www.quadibloc.com/crypto/co040401.htm>

### 5.2. СРЕДСТВА ОБЕСПЕЧЕНИЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

При изучении данной дисциплины используется следующие информационные технологии, программное обеспечение, информационные справочные системы и другие средства, используемые при осуществлении образовательного процесса по дисциплине:

<i>№ n/n</i>	<i>Информационные технологии, включая программное обеспечение, информационные справочные системы и другие используемые средства</i>	<i>Раздел дисциплины</i>	<i>Вид аудиторных занятий и самостоятельной работы</i>
<i>1</i>	<i>Операционная система Windows XP, Borland C++, Microsoft Visual C++ версии 4.0, 5.0, 6.0 MathCAD</i>	<i>1-5</i>	<i>ЛР</i>

### 5.3. РАЗДАТОЧНЫЙ МАТЕРИАЛ

При изучении данной дисциплины раздаточный материал не используется.

## 6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА

При изучении данной дисциплины используются следующее материально-техническое обеспечение:

<i>№ n/n</i>	<i>Наименование и номера специальных* помещений и помещений для самостоятельной работы</i>	<i>Оснащенность специальных помещений и помещений для самостоятельной работы</i>	<i>Раздел дисциплины</i>	<i>Вид контактной работы обучающихся с преподавателем и самостоятельной работы обучающихся</i>
<i>2407</i>		Персональные компьютеры оснащенные программным обеспечением, указанным в пункте 5.2	<i>1-6</i>	<i>ЛР</i>

## 7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Основными видами деятельности обучающегося являются контактная работа с преподавателем и самостоятельная работа, которая включает в себя подготовку к контактной работе обучающихся с преподавателем, проработку материалов, полученных в процессе этой работы, а также подготовку и выполнение всех видов самостоятельной работы, заявленных в рабочей программе дисциплины.

Методика самостоятельной работы предварительно разъясняется преподавателем и в последующем может уточняться с учетом индивидуальных особенностей студентов. Время и место самостоятельной работы выбираются студентами по своему усмотрению с учетом рекомендаций преподавателя.

По зачислении на первый курс или переводу на очередной курс следует провести подготовку к началу обучения. Эта подготовка в самом общем включает несколько необходимых положений:

- Следует убедиться в наличии рабочей программы и необходимых методических указаний по всем видам контактной и самостоятельной работы, указанных в программе дисциплины, понять требования, предъявляемые к изучению дисциплины. При необходимости надлежит получить на кафедре необходимые указания и консультации, контрольные вопросы для изучения дисциплины.
- Необходимо ознакомиться с рейтинговой балльной системой по дисциплине. Преподаватель обязан ознакомить обучающихся с порядком начисления рейтинговых баллов по всем, предусмотренным рабочей программой дисциплины, видам контактной и самостоятельной работы обучающихся.
- Необходимо создать (рационально и эмоционально) максимально высокий уровень мотивации к последовательному и планомерному изучению дисциплины.
- Необходимо изучить список рекомендованной основной и дополнительной литературы и убедиться в её наличии у себя дома или в библиотеке в бумажном или электронном виде.
- Необходимо иметь «под рукой» специальные и универсальные словари и энциклопедии, для того, чтобы постоянно уточнять значения используемых терминов и понятий. Пользование словарями и справочниками необходимо сделать привычкой. Опыт показывает, что неудовлетворительное усвоение предмета зачастую коренится в неточном, смутном или неправильном понимании и употреблении понятийного аппарата учебной дисциплины.
- Желательно в самом начале периода обучения возможно тщательнее спланировать время, отводимое на контактную и самостоятельную работу по дисциплине, представить этот план в наглядной форме и в дальнейшем его придерживаться, не допуская срывов графика индивидуальной работы и аврала в предсессионный период. При этом необходимо руководствоваться Графиком учебного процесса и самостоятельной работы обучающихся по дисциплине, который входит в состав рабочей программы. Пренебрежение этим пунктом приводит к переутомлению и резкому снижению качества усвоения учебного материала.
- Работу следует начинать с изучения рабочей программы, которая содержит основные требования к знаниям, умениям и навыкам обучающихся. Обязательно следует вспомнить рекомендации преподавателя, данные в ходе установочных занятий. Затем – приступить к изучению отдельных разделов и тем в порядке, предусмотренном графиком учебного процесса и самостоятельной работы обучающихся по дисциплине.
- Получив представление об основном содержании раздела, темы, необходимо изучить материал с помощью учебника. Целесообразно составить краткий конспект или схему, отображающую смысл и связи основных понятий данного раздела и включенных в него тем. Затем, как показывает опыт, полезно изучить выдержки из первоисточников.

При желании можно составить их краткий конспект. Обязательно следует записывать возникшие вопросы, на которые не удалось ответить самостоятельно.

**Лекционные занятия** посвящены рассмотрению ключевых, базовых положений дисциплины и разъяснению учебных заданий, выносимых на самостоятельную проработку. Дисциплина построена по модульному принципу, каждый модуль представляет собой логически завершённый раздел курса.

В ходе лекционных занятий конспектировать учебный материал. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов научные выводы и практические рекомендации, положительный опыт. Желательно оставить в рабочих конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Изучение дисциплины следует начинать с проработки настоящей рабочей программы, особое внимание, уделяя целям и задачам, структуре и содержанию курса.

Обучающимся рекомендуется получить в библиотеке учебную литературу по дисциплине, необходимую для эффективной работы на всех видах аудиторных занятий, а также для самостоятельной работы по изучению дисциплины.

Успешное освоение курса предполагает активное, творческое участие студента путем планомерной, повседневной работы.

**Практические и семинарские занятия** проводятся для закрепления усвоенной информации, приобретения навыков ее применения для решения практических задач в предметной области дисциплины.

**Лабораторные работы** предназначены для приобретения опыта практической реализации полученных теоретических знаний. Методические указания к лабораторным работам прорабатываются студентами во время самостоятельной подготовки. Необходимый уровень подготовки контролируется преподавателем перед проведением лабораторных работ.

**Самостоятельная работа** студентов включает проработку лекционного курса, подготовку к практическим, семинарским занятиям и лабораторным работам, выполнение всех заявленных в рабочей программе видов самостоятельной работы (выполнение домашних заданий, расчетно-графических и расчетно-проектировочных работ, курсовых проектов и работ, подготовку к контрольным работам, написание рефератов и пр.). Результаты всех видов работ обучающихся формируются в виде их личных портфолио, которые учитываются на промежуточной аттестации. Самостоятельная работа предусматривает не только проработку материалов лекционного курса, но и их расширение в результате поиска, анализа, структурирования и представления в компактном виде современной информации их всех возможных источников.

В ходе самостоятельной работы необходимо изучить основную литературу, ознакомиться с дополнительной литературой, методическими указаниями по соответствующему виду самостоятельной работы. При этом необходимо учесть рекомендации преподавателя и требования рабочей программы. Очень полезно дорабатывать свой конспект лекции, делая в нем соответствующие записи из литературы, рекомендованной преподавателем и предусмотренной рабочей программой.

Необходимо строго следовать графика учебно-образовательного процесса и самостоятельной работы обучающихся по дисциплине, который входит в состав рабочей программы.

Готовясь, по всем непонятным моментам обращаться за методической помощью к преподавателю. Своевременное и качественное подготовка и выполнение самостоятельной работы базируется на соблюдении настоящих рекомендаций и изучении

рекомендованной литературы. Обучающийся может дополнить список использованной литературы современными источниками, не представленными в списке рекомендованной литературы, и в дальнейшем использовать собственные подготовленные учебные материалы.

Оценивание полученных в процессе изучения дисциплины знаний, умений и навыков проводится в соответствии с Положением о текущем контроле успеваемости и промежуточной аттестации обучающихся МФ МГТУ им. Баумана.

Утвержденные критерии оценки текущего контроля успеваемости и промежуточной аттестации, методика начисления рейтинговых баллов при их прохождении представлены в Фонде оценочных средств по дисциплине, который сформирован как отдельный документ, является приложением к рабочей программе и структурно входит в состав учебно-методического комплекса дисциплины.

**Текущий контроль** проводится в процессе изучения каждого раздела или модуля дисциплины, его итоговые результаты складываются из рейтинговых баллов, полученных при прохождении всех запланированных контрольных мероприятий с учетом своевременности их прохождения, а также посещаемости аудиторных занятий.

Освоение дисциплины, ее успешное завершение на стадии промежуточного контроля возможно только при регулярной работе во время семестра и планомерном прохождении текущего контроля.

Обучающиеся, не выполнившие в полном объеме установленных требований, не допускаются к промежуточной аттестации по данной дисциплине, как не выполнившие график учебного процесса по данной дисциплине.

**Промежуточная аттестация** по результатам семестра по дисциплине проходит в форме, установленной учебным планом, и виде, выбранном преподавателем. При этом проводится проверка освоение ключевых, базовых положений дисциплины, составляющих основу остаточных знаний, умений и навыков по ней.

К промежуточной аттестации допускаются обучающиеся, которые систематически в течение всего семестра работали на занятиях и показали уверенные знания по вопросам, выносившимся на групповые занятия, также выполнившие все виды контактной и самостоятельной работы, предусмотренные рабочей программой дисциплины, прошедшие все контрольных мероприятий и набравшие при этом количество рейтинговых баллов, превышающее установленное рабочей программой минимальное значение.

Непосредственная подготовка к промежуточной аттестации осуществляется по вопросам, представленным в фонде оценочных средств по дисциплине, которые обучающимся должен предоставить преподаватель. Необходимо тщательно изучить формулировку каждого вопроса, вникнуть в его суть, составить план ответа. Обычно план включает в себя:

- показ теоретической и практической значимости рассматриваемого вопроса;
- обзор освещения вопроса;
- определение сущности рассматриваемого предмета;
- основные элементы содержания и структуры предмета рассмотрения;
- факторы, логика и перспективы эволюции предмета;
- показ роли и значения рассматриваемого материала для практической деятельности.

План ответа желательно развернуть, приложив к нему ссылки на первоисточники с характерными цитатами.



## 8. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПРЕПОДАВАТЕЛЮ

При подготовке к контактной работе с обучающимися, контроле текущей успеваемости и промежуточной аттестации обучающихся преподавателю необходимо руководствоваться рабочей программой дисциплины, а также картой обеспеченности литературой, учебно-методической картой, графиком учебного процесса и самостоятельной работы обучающихся по дисциплине, фондом оценочных средств по дисциплине, которые входят в состав рабочей программы.

На первом занятии по дисциплине преподаватель должен довести до обучающихся всю необходимую информацию по дисциплине, предоставить или дать ссылки, на рабочую программу дисциплины, а также карту обеспеченности литературой, учебно-методическую карту, график учебного процесса и самостоятельной работы обучающихся по дисциплине, фонд оценочных средств по дисциплине, все необходимые рекомендации по всем видам контактной и самостоятельной работы, заявленным в рабочей программе дисциплины.

**Лекции** составляют основу теоретической подготовки студентов с целью понимания ими сущности дисциплины и практической работы в бухгалтерских информационных системах.

На лекциях рассматриваются наиболее важные понятия, определяются основные направления дисциплины, дается общая характеристика поставленных вопросов, различные научные концепции, которые есть по данной теме, осмысливаются состояния и перспективы развития, даются особенности использования современных информационных технологий.

Лекции должны активизировать познавательную деятельность обучающихся, вызывать интерес к поставленным проблемам и направлениям развития в профессиональной области, формировать их профессиональный кругозор, аналитические качества, творческий подход к изучению дисциплины, определять направления дальнейшего самостоятельного изучения и практического освоения в данной области.

Изложение материала лекций должно носить проблемный, инновационный характер, способствующий формированию и развитию общекультурных и профессиональных компетенций по профилю обучаемых.

В ходе лекций следует акцентировать внимание на наиболее важных, узловых и сложных в восприятии моментах учебного материала, вовлекая к разрешению сформулированных проблем аудиторию, ставя перед студентами задачи на проведение в ходе внеаудиторной самостоятельной работы аналитических оценок и научных исследований, способствующих закреплению изучаемого материала и постижению нового. Очень важно насытить лекционный материал цифрами и различными практическими примерами, подтверждающими теоретические тезисы. Также следует аргументировано обосновать собственную позицию по спорным теоретическим вопросам. Это способствует активизации мыслительной деятельности обучающихся, повышению их внимания и интереса к материалу лекции, ее содержанию.

Преподавателю, читающему лекции по данной дисциплине, необходимо опираться на основную литературу, представленную в рабочей программе данной дисциплины, а также на учебные пособия, монографии, научные статьи и периодические издания известных специалистов в данной области.

Учебный материал следует излагать с использованием интерактивных методик и презентационных средств, раскрывая новейшие и перспективные информационно-технологические достижения. Если доступен Интернет, то обучающимся можно показать сайты по теме, актуальные страницы с ресурсами.

Определяя задачи на самостоятельную работу студентов, следует обращать внимание обучаемых на использование облачных сред и технологий, обеспечивающих доступ к информационно-технологическим ресурсам из рабочих мест вне учебной базы

университета и филиала.

Контроль усвоения учебного материала, кроме традиционных форм, следует проводить с использованием тематических тестовых заданий, сформулированных в разделе

**Практические занятия и семинары** имеют целью закрепления знаний, полученных на лекциях. Все практические занятия дисциплины проводятся в специализированных классах университета. На первом занятии преподаватель должен напомнить студентам требования техники безопасности.

На практических занятиях студенты овладевают первоначальными профессиональными умениями и навыками, которые в дальнейшем закрепляются и совершенствуются при изучении специальных дисциплин, а также в процессе прохождения производственной практики.

Проводя практические занятия по данной дисциплине, предлагается использовать задания указанные в фонде оценочных средств по данной дисциплине.

Выполнение заданий должно быть индивидуальным. При оценивании выполненных заданий следует учитывать достижение результата, правильность выбора технологии решения, время решения, индивидуальность работы. Веса указанных факторов следует выбирать в зависимости от целей проводимого занятия. Для закрепления практических навыков и умений студентам следует по каждой теме выдавать задания на самостоятельную работу, по трудоемкости сходные с задачами, решаемыми в аудитории.

Наряду с формированием умений и навыков в процессе практических занятий обобщаются, систематизируются, углубляются и конкретизируются теоретические знания, вырабатывается способность и готовность использовать теоретические знания на практике, развиваются аналитические и интеллектуальные умения.

**Лабораторные работы** предназначены для приобретения обучающимися опыта практической реализации полученных теоретических знаний. Методические указания к лабораторным работам должны прорабатываться обучающимися во время самостоятельной подготовки. Перед проведением лабораторных работ преподаватель контролирует необходимый уровень подготовки обучающихся к их выполнению.

**Самостоятельная работа обучающихся** представляет собой индивидуальное выполнение всех видов, заявленных в рабочей программе дисциплины, контактной и самостоятельной работы, которые формируют у обучающегося:

- выработку навыков самостоятельной работы с имеющейся исходной информацией;
- практическую реализацию теоретических знаний с использованием инструментальных средств;
- комплексное применение компетенций, теоретических знаний, практических навыков и умений, приобретенных при изучении данной дисциплины.

При проведении контактных занятий, выдаче материалов и заданий ко всем заявленным видам контактной и самостоятельной работы обучающихся, контроле текущей успеваемости по ним, а также при промежуточной аттестации по дисциплине преподаватель обязан руководствоваться сроками, указанными в учебно-методической карте дисциплины и графике учебного процесса и самостоятельной работы обучающихся по дисциплине. При этом не должно возникать противоречий с утвержденным Положением о текущем контроле успеваемости и промежуточной аттестации обучающихся МФ МГТУ им. Баумана.

При **контроле текущей успеваемости и промежуточной аттестации обучающихся** преподаватель обязан пользоваться оценочными средствами, критериями оценки и начисления рейтинговых баллов, представленных в фонде оценочных средств по данной дисциплине.