МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Мытищинский филиал
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ им. Н.Э. БАУМАНА
(НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)»

Космический факультет

Информационно-измерительные системы и технологии приборостроения (К2)

«УТВЕРЖДАЮ»

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

_____(Макуев В.А.)

(подпись)

« 29 » апреля 2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«ЗАЩИТА ИЗМЕРИТЕЛЬНОЙ ИНФОРМАЦИИ»

Направление подготовки

12.04.01 «Приборостроение»

Направленность подготовки

«Измерительная техника и технологии»

Квалификация выпускника

Магистр

Форма обучения – очная
Срок освоения – 2 года
Курс – II
Семестры – 4
Трудоемкость дисциплины: – 3 зачетных единицы
Всего часов – 108 час.
Из них:
Аудиторная работа – 36 час.
Из них:
Лекции – 6 час.
Практические занятия – 30 час.
Самостоятельная работа – 36 час.
Подготовка к экзамену – 36 час.
Формы промежуточной аттестации:
Экзамен – 4 семестр

Мытищи, 2019г.

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

Автор(ы):

Доцент кафедры К2, к. т. н.		Тарасенко П.А.
(должность, ученая степень, ученое звание)	(подпись)	(Ф.И.О.)
(должность, ученая степень, ученое звание)	(подпись)	(Ф.И.О.)

«6» 04 2019 г.

Рецензент:

Доцент кафедры К1, к. т. н.		Уткин Г.С.
(должность, ученая степень, ученое звание)	(подпись)	(Ф.И.О.)

«6» 04 2019 г.

Рабочая программа рассмотрена и одобрена на заседании кафедры «Информационно-измерительные системы и технологии приборостроения» (К2)

Протокол № 8 *от «* 9 *»* апреля 2019 *г.*

Заведующий кафедрой, д. т. н., профессор		Комаров Е.Г.
(ученая степень, ученое звание)	(подпись)	(Ф.И.О.)

Рабочая программа одобрена на заседании научно-методического совета Космического факультета.

Протокол № 6 *от «* 16 *»* апреля 2019 *г.*

Декан факультета, к.т.н., доцент		Поярков Н.Г.
(ученая степень, ученое звание)	(подпись)	(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		Шевляков А.А.
(ученая степень, ученое звание)	(подпись)	(Ф.И.О.)

С О Д Е Р Ж А Н И Е

ВЫПИСКА ИЗ ОПОП ВО 4
1. ЦЕЛИ ОСВОЕНИЯ И ЗАДАЧИ ДИСЦИПЛИНЫ, ЕЕ МЕСТО В УЧЕБНОМ ПРОЦЕССЕ 4
1.1. Цель освоения дисциплины 4
1.2. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы 4
1.3. Место дисциплины в структуре образовательной программы 6
2. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ 6
3. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ 8
3.1. Тематический план 8
3.2. Учебно-методическое обеспечение для контактной работы обучающихся с преподавателем . . . . .
3.2.1. Содержание разделов дисциплины, объем в лекционных часах 8
3.2.2. Практические занятия и семинары 8
3.2.3. Лабораторные работы 10
3.2.4. Инновационные формы учебных занятий 10
3.3. Учебно-методическое обеспечение для самостоятельной работы обучающихся по дисциплине 10
3.3.1. Расчетно-графические работы и домашние задания 10
3.3.2. Рефераты 11
3.3.3. Контрольные работы 11
3.3.4. Рубежный контроль 11
3.3.5. Другие виды самостоятельной работ 11
3.3.6. Курсовой проект или курсовая работа 11
4. ТЕКУЩИЙ КОНТРОЛЬ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ 11
4.1. Текущий контроль успеваемости обучающихся 11
4.2. Промежуточная аттестация обучающихся 12
5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 12
5.1. Рекомендуемая литература 12
5.1.1. Основная и дополнительная литература 13
5.1.2. Учебные и учебно-методические пособия для подготовки к контактной работе обучающихся с преподавателем и для самостоятельной работы обучающихся 13
5.1.3. Нормативные документы 13
5.1.4. Ресурсы информационно-телекоммуникационной сети «Интернет» и другие электронные информационные источники 13
5.2. Информационные технологии и другие средства, используемые при осуществлении образовательного процесса по дисциплине 13
5.3. Раздаточный материал 14
5.4. Примерный перечень вопросов по дисциплине 14
6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА 15
7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ 15
8. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПРЕПОДАВАТЕЛЮ 18

Выписка из ОПОП ВО по направлению 12.04.01 «Приборостроение» направленность «Информационно-измерительная техника» для учебной дисциплины «Защита измерительной информации»

Индекс	Наименование дисциплины и ее основные разделы	Всего часов
Б1.В.ДВ.03.02	**Защита измерительной информации.** Задачи защиты измерительной информации. Методы и средства реализации. Аппаратные и структурно-организационные методы**.** Теоретические основы и математическая база защиты информации. Криптография, стойкость шифров; абсолютно стойкий шифр, шифры подстановки; шифры перестановки, шифрование с открытым ключом, алгоритм шифрования RSA, теория чисел, группы, кольца, поля	**108**

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

1.1. Цель освоения дисциплины

Цель дисциплины «Защита измерительной информации» входящей в часть, формируемую участниками учебного процесса профессионального цикла состоит в освоении обучающимися теоретических и практических знаний по основным разделам дисциплины и практическом применении их при решении прикладных задач защиты измерительной информации.

В результате освоения учебной дисциплины, обучающиеся приобретают знания, умения навыки обеспечения всесторонней технической подготовки в области касающейся защиты информации и сохранении приватных данных.

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

В результате освоения дисциплины обучающийся должен решать следующие профессиональные задачи в соответствии с видами профессиональной деятельности:
Проектно-конструкторская деятельность:
разработка методик проведения теоретических и экспериментальных исследований по анализу, синтезу и оптимизации характеристик методов и средств защиты измерительной информации в приборостроении.

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**
УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1.1. Анализирует проблемную ситуацию, выделяя ее базовые составляющие, осуществляет поиск вариантов решения на основе доступных источников информации
	УК-1.2. Определяет в рамках выбранного алгоритма вопросы (задачи), подлежащие дальнейшей разработке, предлагает способы их решения
	УК-1.3. Разрабатывает стратегию достижения поставленной цели принимая конкретные решения для ее реализации
ПК-6. Способность разрабатывать программы и их блоки, проводить их отладку и настройку для решения отдельных задач приборостроения	ПК-6.1. Способен разрабатывать алгоритмы программ и их блоков
	ПК-6.2. Реализует отладку и настроечные процедуры для решения отдельных задач приборостроения
ПК-7. Способность контролировать соответствие технической документации разрабатываемых проектов стандартам,	ПК-7.1. Контролирует соответствие разрабатываемых проектов условиям и требованиям технической документации

техническим условиям и другим нормативным документам	ПК-7.2. Анализирует и учитывает соответствие технических и метрологических характеристик проектируемых приборов стандартам, техническим условиям и другим нормативным документам

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)**
УК-1.1. Анализирует поставленную задачу, выделяя ее базовые составляющие, находит и критически оценивает информацию, необходимую для ее решения	Знать: Основы ситуационного анализа решаемых проблем.
	Уметь: Анализировать проблемную ситуацию, выделяя ее основные составляющие.
	Владеть: информацией о методах и вариантах решения .
УК-1.2. Рассматривает возможные варианты решения задачи, оценивая их достоинства и недостатки, грамотно, логично, аргументированно формирует собственные суждения и оценки	Знать: Структуру выбранного алгоритма решения задачи.
	Уметь: Выбирать очередность и приоритетность решения задач подлежащих разработке.
	Владеть: Способами и методами решения.
УК-1.3. Определяет и оценивает последствия возможных решений поставленной задачи	Знать: Цели поставленные при решении данной задачи.
	Уметь: Выбирать оптимальный алгоритм решения по достижению цели.
	Владеть: Методами разработки решения по достижению поставленной цели.
ПК-6.1. Способен разрабатывать алгоритмы программ и их блоков	Знать: Формы представления алгоритмов для разработки программ и блоков.
	Уметь: Определять исходные параметры для разработанных алгоритмов.
	Владеть: Методикой преобразования алгоритмов в соответствующие программы.
ПК-6.2. Реализует отладку и настроечные процедуры для решения отдельных задач приборостроения	Знать: Отладочные и настроечные процедуры для различных средств измерений.
	Уметь: Выполнять практически отладочные и настроечные процедуры для различных приборов.
	Владеть: Методами коррекции погрешностей.
ПК-7.1. Контролирует соответствие разрабатываемых проектов условиям и требованиям технической документации	Знать: Основные требования технической документации на разработанные проекты.
	Уметь: Сопоставить параметры и требования технических характеристик, полученным реально, при воплощении в жизнь проекта.
	Владеть: Методами принятия решений по соответствию разрабатываемых проектов условиям и требованиям технической документации.
ПК-7.2. Анализирует и учитывает соответствие технических и метрологических характеристик проектируемых приборов стандартам, техническим условиям и другим нормативным документам	Знать: Требования стандартов на технические и метрологические характеристики разрабатываемых приборов.
	Уметь: Проводить сравнение технических и метрологических характеристик проектируемых приборов стандартам и другим нормативным документам.
	Владеть: Представлением о системе

	стандартов технических условий и других нормативных документах.

1.3. Место дисциплины в структуре образовательной программы

Данная дисциплина входит в часть Б1.В, формируемую участниками образовательного процесса и участвует в формировании профилизации по направленности «информационно-измерительная техника и технологии».

Изучение данной дисциплины базируется на знаниях, умениях и навыках, полученных при изучении дисциплин «Информационные технологии в приборостроении» и «Программное обеспечение измерительных процессов».

Полученные при изучении данной дисциплины знания, умения и навыки будут использоваться при изучении следующих дисциплин: «Системы измерений параметров физических сред»

2. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Объем дисциплины: в зачетных единицах – 3 з.е., в академических часах –108 час.

Вид учебной работы	Часов		Семестры
	всего	в том числе в иннова-ционных формах	4
Общая трудоемкость дисциплины:	**108**	**6**	**108**
Аудиторная работа обучающихся с преподавателем:	**36**	**6**	**36**
Лекции (**Л**)	6	2	6
Практические занятия (**Пз**) *и(или)* семинары (**С**)	30	4	30
Лабораторные работы (**Лр**)	-		-
Самостоятельная работа обучающихся:	**36**	**-**	**36**
Проработка прослушанных лекций и учебного материала, перенесенного с аудиторных занятий на самостоятельную проработку, изучение рекомендуемой литературы (**Л**) – _	1,5	-	1,5
Подготовка к практическим занятиям (**Пз**) *и(или)* семинарам (**С**) – _	7,5	-	7,5
Подготовка к лабораторным работам (**Лр**) – _	-	-	-
Выполнение расчетно-графических (**РГР**) *и(или)* домашних заданий (**Дз**) – _	18	-	18
Выполнение других видов самостоятельной работы (**Др**) – _	9	-	9
Подготовка к экзамену: *(только при наличие экзамена(ов) – по **36** час на 1 экзамен)*	**36**	**-**	**36**
Форма промежуточной аттестации: *(зачет (**Зач**), дифференцированный зачет (**ДЗач**), экзамен (**Э**))*	Э	-	Э

3. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1. Тематический план

№	Раздел дисциплины	Аудиторные занятия			Самостоятельная работа студента и формы ее контроля	
		Л, часо	№ Пз (С)	№ Лр	№ ДЗ	№ Кр
1	Задачи защиты измерительной информации. Методы и средства реализации. Аппаратные и структурно-организационные методы	1	1;2			
2	Теоретические основы и математическая база защиты информации.	1	3;4;5			
3	Основы теории чисел. Алгебра.	1	6;7;8			
4	Криптография	1	9;10		1	
5	Шифрование с открытым ключом	1	11;12			
6	Целочисленная арифметика многократной точности.	1	13;14; 15			

3.2. Учебно-методическое обеспечение для контактной работы

обучающихся с преподавателем

3.2.1. Содержание разделов дисциплины, объем в лекционных часах (Л) – 6 часов

№ Л	Раздел дисциплины и его содержание	Объем часов
1	Задачи защиты измерительной информации. Методы и средства реализации. Аппаратные и структурно-организационные методы	1
2	Теоретические основы и математическая база защиты информации.	1
3	Основы теории чисел. Алгебра.	1
4	Криптография	1
5	Шифрование с открытым ключом	1
6	Целочисленная арифметика многократной точности.	1

3.2.2. Практические занятия (Пз) или семинары (С) – 30 часов

№ Пз	Тема практического занятия и его содержание	Объем часов	Раздел дисциплины	Виды контроля Текущей успеваимости
1	Задачи защиты измерительной информации. Методы и средства реализации. Аппаратные и структурно-организационные методы	2	1	Устное и письменное тестирование
2	Задачи защиты измерительной информации. Методы и средства реализации. Аппаратные и структурно-организационные методы.	2	1	Устное и письменное тестирование

№ Пз	Тема практического занятия и его содержание	Объем часов	Раздел дисциплины	Виды контроля Текущей успеваимости
3	Теоретические основы и математическая база защиты информации.	2	2	Устное и письменное тестирование
4	Теоретические основы и математическая база защиты информации.	2	2	Устное и письменное тестирование
5	Теоретические основы и математическая база защиты информации.	2	2	Устное и письменное тестирование
6	Основы теории чисел. Алгебра.	2	3	Устное и письменное тестирование
7	Основы теории чисел. Алгебра.	2	3	Устное и письменное тестирование
8	Основы теории чисел. Алгебра.	2	3	Устное и письменное тестирование
9	Криптография	2	4	Устное и письменное тестирование
10	Криптография	2	4	Устное и письменное тестирование
11	Шифрование с открытым ключом	2	5	Устное и письменное тестирование
12	Шифрование с открытым ключом	2	5	Устное и письменное тестирование
13	Целочисленная арифметика многократной точности.	2	6	Устное и письменное тестирование
14	Целочисленная арифметика многократной точности.	2	6	Устное и письменное тестирование
15	Целочисленная арифметика многократной точности.	2	6	Устное и письменное тестирование

3.2.3. Лабораторные работы (Лр) - 0 часов.

Лабораторные работы учебным планом не предусмотрены.

3.2.4. Инновационные формы учебных занятий

При изучении данной дисциплины применяются следующие инновационные формы учебных занятий:

- интерактивная лекция;
- работа в команде (в группах);
- выступление студента в роли обучающего.

При этом предусматривается использование таких вспомогательных средств, как мультимедийный проектор, плакаты, раздаточный материал.

3.3. Учебно-методическое обеспечение для самостоятельной работы обучающихся по дисциплине

На самостоятельную работу обучающихся, согласно учебному плану, отводится – 36 часов.

Самостоятельная работа студентов включают в себя:

- Проработку прослушанных лекций, учебного материала, перенесенного с аудиторных занятий на самостоятельную проработку, изучение рекомендованной литературы – 1.5 часов.
- Подготовку к практическим занятиям – 7,5 часа.
- Подготовку домашнего задания – 18 часов.
- Выполнение других видов самостоятельной работы – 9 часов.

Часы, выделенные по учебному плану, на подготовку к экзамену в общее количество часов на самостоятельную работу обучающихся не входит, а выносится на недели, отведенные на сессии − 36 часов на один экзамен.

Часы на внеаудиторные виды контактной работы обучающихся с преподавателем выделяются из самостоятельной работы обучающихся и часов, выделенных на экзамен, в соответствии с нормативами нагрузки преподавателей, утверждаемыми в университете ежегодно.

3.3.1. Расчётно-графические работы (РГР) домашние задания (Дз) – 18 часов

. Выполняется одна домашняя работа

№ ДЗ	Тема домашнего задания	Объем часов	Раздел дисциплины
1	Нахождение обратной величины числа *n* по модулю *k* по модулю. Функция Эйлера.	18	4-6

3.3.2. Рефераты – 0 часов

Рефераты рабочей программой не предусмотрены

3.3.3 Контрольные работы (Кр) – 0 часов

Контрольные работы рабочей программой не предусмотрены

3.3.4. Рубежный контроль – 0 часов

Рубежный контроль рабочей программой не предусмотрен

3.3.5. Другие виды самостоятельной работы (Др) – 27 часов

Другие виды самостоятельной работы относятся к нерегламентированной самостоятельной работе обучающихся, связанной с углубленным изучением отдельных тем или разделов дисциплины, их творческой деятельностью, развитием личностных качеств и т.д. Конкретные формы других видов самостоятельной работы обучающийся выбирает самостоятельно или по рекомендации преподавателя в ходе изучения дисциплины.

3.3.6. 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

Оценочные средства по всем заявленным в рабочей программе видам аудиторных занятий 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.

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.)
4 семестр				
1	10	Проверка домашнего задания № 1	УК-1; ПК-6; ПК-7	30/63
2	1-10	Контроль посещаемости (14 занятий)		0/7
		Всего за модуль		**30/70**

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	1-10	**Экзамен**	**да**	**10/30**
Итого:				**40/100**

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. Садовничего, 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. Ресурсы информационно-телекоммуникационной сети «Интернет» и другие электронные информационные источники

1. http://e.lanbook.com/ – Электронно-библиотечная система издательства «Лань».
2. http://bkp.mgul.ac.ru/MarcWeb/ – Электронный каталог библиотеки МФ МГТУ им. Н.Э. Баумана
3. http://www.msfu.ru/info/cdo/ – сайт СДО МФ МГТУ им. Н.Э. Баумана (для зарегистрированных пользователей).

Основная и дополнительная литература, учебные и учебно-методические пособия для подготовки к аудиторной работе обучающихся с преподавателем и для самостоятельной работы обучающихся, нормативные документы, ресурсы информационно-телекоммуникационной сети «Интернет» и другие электронные информационные источники, необходимые для освоения дисциплины, их количество и наличие в библиотеке, ЭБС, на кафедре, распределение по разделам (темам) дисциплины, всем запланированным видам аудиторной работы обучающихся с преподавателем и самостоятельной работе обучающихся, представлены в карте обеспеченности

литературой, которая сформирована как отдельный документ и является приложением к рабочей программе.

5.2. Информационные технологии и другие средства, используемые при осуществлении образовательного процесса по дисциплине

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

№ п/п	Информационные технологии, включая программное обеспечение, информационные справочные системы и другие используемые средства	Раздел дисциплины	Вид аудиторных занятий и самостоятельной работы
1	Электронно-библиотечная система издательства «Лань» (электронная учебная, методическая и научная литература по тематике дисциплины)	1-6	Л, Пз и ДЗ1
2	Электронные издания Издательства МГТУ им. Н. Э. Баумана (электронная учебная, методическая и научная литература по тематике дисциплины)	1-6	Л, Пз и ДЗ1
3	Электронный каталог библиотеки МФ МГТУ им. Н.Э. Баумана (учебная, методическая и научная литература по тематике дисциплины)	1-6	Л, Пз и ДЗ1
4	Электронная образовательная среда МФ МГТУ им. Н.Э. Баумана (для обеспечения учебно-методическими материалами, проверки знаний студентов по различным разделам дисциплины, подготовленности их к проведению и защите лабораторных работ)	1-6	Л, Пз и ДЗ1
5	Операционная система Windows XP,Borland C++,Microsoft Visual C++ версии 4.0, 5.0,6.0 MathCAD	1-6	Л, Пз и ДЗ1

5.3. Раздаточный материал

При изучении данной дисциплины используются следующий раздаточный материал:

№ п/п	Раздаточный материал	Раздел дисциплины	Вид аудиторных занятий
1	Виды аппаратной реализации цифровых фильтров	1-6	Л, Пз

5.4. Примерный перечень вопросов к экзамену по учебной дисциплине.

При проведении промежуточного контроля, для оценки результатов изучения дисциплины вынесены следующие вопросы:

1. Теория чисел; сравнения; НОД;
2. Теория чисел; алгоритм Евклида;
3. Теория чисел; непрерывная дробь; подходящие дроби.

4. Нахождение обратной величины по модулю; функция Эйлера;
5. Теорема Эйлера;
6. Теорема Ферма; символ Лежандра;
7. Алгебра; группа, порядок группы; подгруппа; циклическая группа; теорема Лагранжа;
8. Алгебра; теорема Лагранжа;
9. Кольца; примеры колец;
10. Кольцо Zm, делители нуля;
11. Поля; примеры полей; поле Галуа GF(q); мультипликативная группа поля Галуа;
12. Примитивный элемент, расширения полей, подполя, характеристика пол.
13. Стойкость шифров; абсолютно стойкий шифр; проблема распространения ключей; шифр Цезаря;
14. Криптография; исторические примеры шифров;
15. Стойкость шифров; абсолютно стойкий шифр; проблема распространения ключей; шифр Цезаря;
16. Потоковые шифры;
17. Блочные шифры; симметрические шифросистемы;
18. Шифрование с открытым ключом; односторонняя функция; функция с секретом; схема Диффи-Хеллмана;
19. Электронная подпись; протокол аутентификации; протокол подбрасывания монеты по телефону; электронное голосование; электронные торги;
20. Электронное голосование; электронные торги;
21. Целочисленная арифметика многократной точности; расширенный двоичный НОД;
22. Целочисленная арифметика многократной точности сложение, вычитание, умножение, возведение в степень слева-направо и справа-налево;
23. Задачи защиты измерительной информации. Методы и средства реализации;
24. Аппаратные и структурно-организационные методы и средства защиты измерительной информации.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА

При изучении данной дисциплины используются следующее материально-техническое обеспечение:

№ п/п	Наименование специальных* помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы	Раздел дисципли-ны	Вид аудиторных занятий и самостоятель-ной работы студентов
1	лаборатория 332	. Персональные компьютеры оснащенные программным обеспечением, указанным в пункте 5.2	1-6	Пз и ДЗ1

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 бальной 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 – приступать 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 завершенный 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 учебного 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 входит 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.