МИНОБРНАУКИ РОССИИ
АСТРАХАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

СОГЛАСОВАНО	УТВЕРЖДАЮ
Руководитель ОПОП	Заведующий кафедрой ИБиЦТ
_____ И.М. Ажмухамедов	_____ А.Н. Марьенков
_____	протокол заседания кафедры № 11
«3» июня 2021 г.	от «3» июня 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Математические основы защиты информации

наименование

Составитель(-и)	**Выборнова О.Н., к.т.н, доцент кафедры информационной безопасности и цифровых технологий** **Мартьянова А.Е., к.т.н., доцент кафедры информационной безопасности и цифровых технологий**
Направление подготовки / специальность	**10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**
Направленность (профиль) ОПОП	**«Организация и технология защиты информации»**
Квалификация (степень)	**бакалавр**
Форма обучения	**очная**
Год приема	**2021**
Курс	**1,2**

Астрахань – 2021

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.1. Целями освоения дисциплины (модуля) «Математические основы защиты информации» являются - изучение основных понятий, утверждений и методов, играющих фундаментальную роль в моделировании процесса выработки решений, решение разнообразных теоретических и практических задач, возникающих при передаче и хранении информации.

1.2. Задачи освоения дисциплины (модуля):

- научить студентов проводить проектные расчеты элементов систем обеспечения информационной безопасности;
- подготовить студентов к проведению экспериментов по заданной методике, к обработке и анализу их результатов.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОПОП

2.1. Учебная дисциплина (модуль) «Математические основы защиты информации» относится к базовой части учебного плана направления подготовки 10.03.01 Информационная безопасность 2021 года набора, изучается во 2 и 3 семестрах.

2.2. Для изучения данной учебной дисциплины (модуля) необходимы следующие знания, умения и навыки, формируемые предшествующими дисциплинами:

- Математика;
- Информатика.

Знания: основ элементарной математики.

Умения: работать с координатной плоскостью, составлять и решать уравнения, системы уравнений, неравенства.

Навыки: самостоятельной работы с учебной литературой, применения математических навыков в смежных областях.

2.3. Перечень последующих учебных дисциплин, для которых необходимы знания, умения и навыки, формируемые данной учебной дисциплиной:

- Теория информации;
- Теория принятия решений и методы оптимизации;
- Криптографические методы защиты информации;
- Криптографические протоколы;
- Теория вероятностей и математическая статистика.

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

Процесс изучения дисциплины «Математические основы защиты информации» направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО и ОПОП ВО по данному направлению подготовки (специальности):

а) общепрофессиональных (ОПК):

ОПК-3 - способен использовать необходимые математические методы для решения задач профессиональной деятельности; ОПК-11 - способен проводить эксперименты по заданной методике и обработку их результатов; ОПК-12 - способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений.

Таблица 1.
Декомпозиция результатов обучения

Код компетенции	Планируемые результаты освоения дисциплины (модуля)		
	Знать (1)	Уметь (2)	Владеть (3)
ОПК-3	ОПК-3.1. Знать: основы математики, основные математические методы.	ОПК-3.2. Уметь: решать стандартные профессиональные задачи с применением методов математического анализа и моделирования.	ОПК-3.3. Владеть: навыками математического исследования объектов профессиональной деятельности.
ОПК-11	ОПК-11.1. Знать: методику проведения экспериментов.	ОПК-11.2. Уметь: уметь решать задачи вычислительного и теоретического характера, проводить эксперименты.	ОПК-11.3. Владеть: методами корректной оценки погрешностей измерений и расчетов.
ОПК-12	ОПК-12.1. Знать: основные исходные данные для проектирования подсистем.	ОПК-12.2. Уметь: проводить экспериментальные исследования и проектировать подсистемы и средств обеспечения защиты информации.	ОПК-12.3. Владеть: методами технико-экономического обоснования соответствующих проектных решений.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Объем дисциплины (модуля) «Математические основы защиты информации» в зачетных единицах **10* зачетных единиц** (2й семестр –4 ЗЕ, 3й семестр – 6 ЗЕ). Всего 360 часов: 108 часов выделено на контактную работу обучающихся с преподавателем (36 часов – лекции, 72 часа – лабораторные работы), 252 часов – на самостоятельную работу обучающихся/

Таблица 2.
Структура и содержание дисциплины (модуля)

№ п/п	Наименование радела (темы)	Семестр	Неделя семестра	Контактная работа (в часах)			Самостоят. работа		Формы текущего контроля успеваемости *(по неделям семестра)* Форма промежуточной аттестации *(по семестрам)*
				Л	ПЗ	ЛР	КР	СР	
1	Матрицы и системы линейных алгебраических уравнений	2	1-4	6		12		30	Сдача типового расчета «Матрицы и системы линейных алгебраических уравнений». Опрос на экзамене
2	Векторная алгебра		5-10	4		8		30	Сдача типового расчета «Векторная алгебра». Опрос на экзамене
3	Прямая и плоскость		11-15	4		8		15	Написание контрольной работы «Прямая и плоскость». Опрос на экзамене

4	Линии и поверхности второго порядка		16-18	4		8		15	Сдача типового расчета «Линии и поверхности второго порядка». Опрос на экзамене
	Итого за 2 семестр			**18**		**36**		**90**	**ЭКЗАМЕН**
5	Целые числа и основы теории делимости	3	1-4	6		12		39	Сдача типового расчета «Целые числа и основы теории делимости». Отчет по лабораторным работам «Алгоритм Евклида», «Простые числа». Опрос на экзамене
6	Основы теории сравнений		5-10	4		8		39	Написание контрольной работы «Основы теории сравнений». Опрос на экзамене
7	Алгебраические структуры		11-15	4		8		39	Сдача типового расчета «Алгебраические структуры». Опрос на экзамене
8	Многочлены		16-18	4		8		45	Написание контрольной работы «Многочлены». Опрос на экзамене
	Итого за 3 семестр			**18**		**36**		**162**	**ЭКЗАМЕН**
	ИТОГО		**360**	**36**		**72**		**252**	

Условные обозначения:

Л – занятия лекционного типа; ПЗ – практические занятия, ЛР – лабораторные работы; КР – курсовая работа; СР – самостоятельная работа по отдельным темам

Таблица 3.

Матрица соотнесения тем/разделов учебной дисциплины/модуля и формируемых в них компетенций

Темы, разделы дисциплины	Кол-во часов	Компетенции			
		ОПК-3	ОПК-11	ОПК-12	общее количество компетенций
Матрицы и системы линейных алгебраических уравнений	48	+	+	+	3
Векторная алгебра	42	+	+	+	3
Прямая и плоскость	27	+	+	+	3
Линии и поверхности второго порядка	27	+	+	+	3
Целые числа и основы теории делимости	57	+	+	+	3
Основы теории сравнений	51	+	+	+	3
Алгебраические структуры	51	+	+	+	3

Многочлены	57	+	+	+	3
Итого	360				

Содержание дисциплины

2 семестр

1. Матрицы и системы линейных алгебраических уравнений

Определение понятия матрица, определитель, минор, алгебраическое дополнение. Действия над матрицами. Расчет обратной матрицы. Вычисление ранга.

Система n линейных уравнений с n неизвестными. Однородная и неоднородная системы. Решение по правилу Крамера. Решение с помощью обратной матрицы. Метод Гаусса. Критерий совместности. Теорема Кронекера-Капелли. Фундаментальные решения однородной СЛУ, свойства. Связь между общими решениями однородной и неоднородной систем.

2. Векторная алгебра

Элементы векторной алгебры. Основные понятия. Линейные операции над векторами.

Декартова система координат. Скалярное произведение векторов. Векторное и смешанное произведение векторов.

Линейная зависимость векторов. Базис. Координаты вектора в данном базисе. Преобразование координат векторов при замене базиса.

3. Прямая и плоскость

Уравнение линии на плоскости. Уравнение прямой на плоскости. Уравнение прямой по точке вектора и нормали. Уравнение прямой, проходящей через две точки. Уравнение прямой по точке и угловому коэффициенту. Уравнение прямой по точке и направляющему вектору. Уравнение прямой в отрезках. Нормальное уравнение прямой. Взаимное расположение прямых на плоскости.

Общее уравнение плоскости. Исследование общего уравнения плоскости. Уравнение плоскости, проходящей через три точки. Уравнение плоскости в отрезках. Нормальное уравнение плоскости. Расстояние от точки до плоскости. Взаимное расположение двух плоскостей. Угол между плоскостями. Условия параллельности и перпендикулярности двух плоскостей.

Уравнение линии в пространстве. Параметрические уравнения прямой. Канонические уравнения прямой. Уравнение прямой, проходящей через две точки. Задание прямой двумя общими уравнениями. Углы между двумя прямыми. Условия параллельности и перпендикулярности двух прямых. Взаимное расположение двух прямых в пространстве. Расстояние от точки до прямой в пространстве. Взаимное расположение прямой и плоскости. Угол между прямой и плоскостью. Условия параллельности и перпендикулярности прямой и плоскости.

4. Линии и поверхности второго порядка

Кривые второго порядка. Окружность. Эллипс. Гипербола. Парабола.

Системы координат. Полярная система координат.

Поверхности второго порядка. Цилиндрические поверхности. Поверхности вращения. Трехосный эллипсоид. Однополосный гиперболоид. Двухполосный гиперболоид. Эллиптический гиперболоид. Гиперболический параболоид.

3 семестр

5. Целые числа и основы теории делимости

Делимость целых чисел. Свойства делимости. Теорема о делении с остатком.

Наибольший общий делитель. Алгоритм Евклида. Цепные дроби. Скобки Эйлера. Наименьшее общее кратное.

Простые числа. Критерий простоты числа. Решето Эратосфена. Разложение чисел на простые множители. Основная теорема арифметики.

6. Основы теории сравнений

Определение и свойства сравнений. Критерий сравнимости

Полная система вычетов по модулю. Функция Эйлера. Приведенная система вычетов по модулю.

Теорема Эйлера. Теорема Ферма.

Сравнения первой степени. Методы решения сравнений. Системы сравнений. Китайская теорема об остатках.

7. Алгебраические структуры

Алгебраические операции, заданные на множестве.

Группы, конечные абелевы группы. Подгруппы. Теорема Лагранжа. Нормальный делитель группы. Факторгруппа. Циклические группы.

Кольца. Подкольца. Идеал кольца. Факторкольцо.

Поле. Подполе.

8. Многочлены

Кольцо многочленов от одной переменной над кольцом. Вопрос делимости в кольце. НОД, НОК многочленов.

Неприводимые над полем многочлены. Разложение многочленов.
Корни многочленов. Теорема Безу. Поле разложения многочлена. Теорема Кронекера. Схема Горнера.

5. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

5.1. Указания по организации и проведению лекционных, практических (семинарских) и лабораторных занятий с перечнем учебно-методического обеспечения:

Методические указания к организации и проведению лекций.

Лекционное занятие по математическим дисциплинам представляет собой систематическое, последовательное, монологическое изложение преподавателем-лектором учебного материала, теоретического и практического характера. Такое занятие представляет собой элемент технологии представления учебного материала путем логически стройного, систематически последовательного и ясного, доступного для понимания изложения.

Главной задачей лектора является функция организации процесса познания студентами материала изучаемой дисциплины на всех этапах ее освоения, предусмотренной государственным образовательным стандартом.

При подготовке к лекции особое внимание следует обращать на решение следующих организационно-методических вопросов:

1. Определение основной цели лекции, ее главной идеи. Цель задается требованиями учебной программы, местом лекции в изучаемом курсе (дисциплин) и самим названием. Цель и содержание лекции, даже при одной и той же формулировке темы, могут и должны различаться при чтении слушателям разного уровня обучения и разных категорий: первоначальная подготовка, переподготовка, повышение квалификации, студенты разных факультетов и т.д. Поэтому целесообразно начинать подготовку лекции с постановки перед собой вопроса о том, для какой категории слушателей необходима данная лекция и какой конкретно материал необходимо включить в ее текст, чтобы аудитория была способна его воспринимать. Ответив на поставленные вопросы, преподаватель конкретизирует содержание лекции.

2. Объем материала, входящего в содержание лекции.

Практика показывает, что у преподавателя, готовящегося к лекции, как правило, бывает запланировано материала значительно больше, чем его можно изложить за отведенное время. Следовательно, надо отобрать самое важное для достижения поставленной цели лекции. Для определения объема лекции можно использовать следующий методический прием: нужно прочитать вслух подготовленный текст лекции, замерив время, а затем увеличить это время примерно на 20-30%. Как показывает практика, столько времени будет затрачено при чтении

лекции в аудитории. Безусловно, при определении объема содержания лекции необходимо ориентироваться на требования учебной программы.

3. Детальная проработка структуры лекции.

Для формирования структуры лекции необходимо тему лекции разбить на подвопросы и сформулировать название последних. Это обеспечивает более строгое подчинение материала теме и цели лекции, позволяет лучше отобрать материал и логичнее его расположить, наметить план лекции.

4. Разработка текста лекции.

При работе над текстом лекции преподаватель должен подумать над тем, как повысить научность и практическую значимость лекции, реализовать все ее функции, как лучше скомпоновать материал, при этом, не забывая о принципе доступности излагаемого материала.

Нельзя превращать лекцию в чтение текста. Текст лекции должен вести, направлять внимание, обеспечивать активность студентов на занятии, вовлекать их в научную беседу.

5. Наглядность и практический материал.

Подготовка средств наглядности и практического материала (образцов решения типовых задач по материалу лекции) – важный элемент в подготовке лекции. Наглядность помогает студентом понять смысл изучаемых понятий и теорем, образцы решения типовых задач демонстрируют применение теоретического материала лекции к решению практических заданий. При подготовке к лекции преподавателю необходимо продумать, какие теоретические аспекты лекции будут сопровождаться наглядностью и примерами решения задач, и подобрать соответствующие материалы.

6. Непосредственный психологический настрой преподавателя на чтение лекции.

Психологи считают, что каждый преподаватель перед встречей с аудиторией (слушателями) должен подготовить себя к этому как морально, так и физически. Перед началом учебного занятия следует отдохнуть и сосредоточиться. Еще раз мысленно представить план занятия, продумать наиболее ответственные моменты из текста лекции, можно проговорить их про себя или вслух. Надо отбросить все, не имеющее отношения к теме занятия; целиком переключиться на предстоящее выступление. Это будет способствовать снятию психологического напряжения и преодолению излишнего волнения.

При проведении лекции всегда следует помнить, что лекция имеет четкую структуру, включающую в себя: введение, основную часть и заключение. В каждом из ее элементов преподавателю следует соблюдать определенные действия и правила поведения, суть которых и определяет методику чтения лекции.

Во введении к числу основных действий преподавателя можно отнести:

1. Объявление темы и плана лекции, указание основной и дополнительной литературы.
2. Разъяснение целей занятия и способов их достижения.
3. Обозначение места лекции в программе и ее связь с другими дисциплинами.
4. Создание рабочей обстановки в аудитории, вызвать у слушателей интерес к изучаемой теме.

В основной части лекции преподавателю следует применить следующие методические приемы:

1. Установление контакта с аудиторией.
2. Убежденное и эмоциональное изложение материала.
3. Установление четких временных рамок на изложение материала по намеченному плану.
4. Использование материала лекции как опорного для лучшего усвоения изучаемой дисциплины.
5. Контроль за грамотностью своей речи и поведением.
6. Наблюдение за аудиторией и поддержание с ней контакта на протяжении всего занятия.

В заключительной части лекции преподавателю рекомендуется:

1. Подвести итоги сказанного в основной части и сделать выводы по теме.

2. Ответить на вопросы студентов.

3. Напомнить студентам о методических указаниях по организации самостоятельной работы.

4. Объявить в аудитории очередную тему занятий и порекомендовать присутствующим ознакомиться с ее основным содержанием.

5. Отметить присутствующих на лекции.

При подготовке к лекциям рекомендуется использовать литературу, указанную в пункте 8.

Методические указания к организации и проведению лабораторных занятий.

Целью лабораторных занятий является формирование у студентов умений и навыков применять материал лекции при решении математических задач, повышение знаний студентов, совершенствование навыков изложения своих мыслей устно и письменно, навыков работы с математической литературой, умения осуществлять поиск решения задачи и анализировать полученные результаты.

Состав заданий для лабораторной работы и практического занятия должен быть спланирован с расчетом, чтобы за отведенное время они могли быть выполнены качественно большинством обучающихся.

Содержание лабораторных работ и практических занятий по учебной дисциплине, междисциплинарному курсу должно охватывать весь круг профессиональных умений, на подготовку к которым ориентирована данная дисциплина, а в совокупности по всем учебным дисциплинам охватывать всю профессиональную деятельность, к которой готовится специалист.

При планировании состава и содержания лабораторных работ и практических занятий следует исходить из того, что они имеют разные ведущие дидактические цели.

Ведущей дидактической целью лабораторных работ является экспериментальное подтверждение и проверка существенных теоретических положений (законов, зависимостей), поэтому они занимают преимущественное место при изучении дисциплин профессионального цикла.

При выборе содержания и объема лабораторных работ следует исходить из сложности учебного материала для усвоения, из внутрипредметных и межпредметных связей, из значимости изучаемых теоретических положений для предстоящей профессиональной деятельности, из того, какое место занимает конкретная работа в совокупности лабораторных работ и их значимости для формирования целостного представления о содержании учебной дисциплины.

При планировании лабораторных работ и практических занятий следует учитывать, что в ходе выполнения заданий у обучающихся формируются практические умения и навыки обращения с различными приборами, установками, лабораторным оборудованием, аппаратурой, которые могут составлять часть профессиональной практической подготовки, а также исследовательские умения: наблюдать, сравнивать, анализировать, устанавливать зависимости, делать выводы и обобщения, самостоятельно вести исследование, оформлять результаты.

Лабораторная работа как вид учебного занятия должна проводиться в специально оборудованных учебных лабораториях. Продолжительность лабораторной работы - не менее двух академических часов. Необходимыми структурными элементами лабораторной работы, помимо самостоятельной деятельности обучающихся, являются инструктаж, проводимый преподавателем, а также организация обсуждения итогов выполнения лабораторной работы.

Выполнению лабораторных работ и практических занятий предшествует проверка знаний обучающихся - их теоретической готовности к выполнению задания.

Лабораторные занятия могут носить репродуктивный, частично-поисковый и поисковый характер.

Работы, носящие репродуктивный характер, отличаются тем, что при их проведении обучающиеся пользуются подробными инструкциями, в которых указаны: цель работы,

пояснения (теория, основные характеристики), оборудование, аппаратура, материалы и их характеристики, порядок выполнения работы, таблицы, выводы (без формулировки), контрольные вопросы, учебная и специальная литература.

Работы, носящие частично-поисковый характер, отличаются тем, что при их проведении обучающиеся не пользуются подробными инструкциями, им не дан порядок выполнения необходимых действий, и они требуют от обучающихся самостоятельного подбора оборудования, выбора способов выполнения работы в инструктивной и справочной литературе и др.

Работы, носящие поисковый характер, характеризуются тем, что обучающиеся, опираясь на имеющиеся у них теоретические знания, должны решить новую для них проблему.

При планировании лабораторных занятий необходимо находить оптимальное соотношение репродуктивных, частично-поисковых и поисковых работ, чтобы обеспечить высокий уровень интеллектуальной деятельности.

Формы организации обучающихся при проведении лабораторных работ и практических занятий - фронтальная, групповая и индивидуальная.

При фронтальной форме организации занятий все обучающиеся выполняют одновременно одну и ту же работу.

При групповой форме организации занятий одна и та же работа выполняется группами по 2 - 5 человек.

При индивидуальной форме организации занятий каждый обучающийся выполняет индивидуальное задание.

Лабораторные работы выполняются учащимися на персональных компьютерах.

На лабораторных занятиях студенты овладевают основными методами и приемами самостоятельного решения задач. Если студент не может самостоятельно разобраться в решении той или иной задачи преподавателю рекомендуется дать консультацию, пояснить еще раз метод решения и далее стимулировать работу студента путем системы наводящих вопросов при решении аналогичных задач.

Лабораторные занятия должны так быть организованы, чтобы студенты ощущали нарастание сложности выполнения заданий, испытывали бы положительные эмоции от переживания собственного успеха в учении.

При подготовке к занятию, разработке заданий и плана занятия преподаватель должен учитывать уровень подготовленности и интересы каждого студента группы, выступая в роли консультанта и координатора, не подавляя его самостоятельности и инициативы.

При подготовке к лабораторным занятиям рекомендуется использовать учебно-методическое обеспечение, указанное в пункте 8.

5.2. Указания для обучающихся по освоению дисциплины (модулю) «Математические основы защиты информации».

Приступая к изучению учебной дисциплины «Математические основы защиты информации», студентам необходимо ознакомиться с учебной программой дисциплины, учебной, научной и методической литературой, рекомендуемой для ее изучения, получить в библиотеке рекомендованные учебники, учебно-методические пособия, завести новую тетрадь для конспектирования лекций и выполнения практических заданий.

В ходе лекционных занятий студенту рекомендуется вести конспектирование учебного материала. Желательно оставить в рабочих конспектах поля, на которых можно делать пометки о рекомендованной литературе, дополняющей материал прослушанной лекции. В случае неясности материала лекции, студент может задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций. Студент может дорабатывать свой конспект лекции, делая в нем соответствующие записи из литературы, рекомендованной преподавателем и предусмотренной учебной программой.

При подготовке к лабораторным занятиям студент должен изучить лекционный материал. Необходимо запомнить основные понятия, теоремы лекции и изучить методы решения типовых задач, это должно стать основным ориентиром во всех последующих видах работы с лекциями и учебным материалом.

При подготовке к контрольной работе и экзамену рекомендуется повторять пройденный учебный материал в строгом соответствии с учебной программой, примерным перечнем учебных вопросов, задач, выносящихся на контрольную работу, зачет, экзамен. Студенту необходимо обратить особое внимание на темы учебных занятий, пропущенные им по разным причинам. При необходимости обратиться за консультацией и методической помощью к преподавателю. За каждое пропущенное занятие, независимо от причины пропуска, следует отчитаться перед преподавателем, взяв предварительно задание.

Кроме лекций и лабораторных занятий по дисциплине «Математические основы защиты информации» учебным планом предусмотрена, и самостоятельная работа студента по изучению этой дисциплины.

Самостоятельная работа – это планируемая работа студентов, выполняемая по заданию и при методическом руководстве преподавателя, но без его непосредственного участия. Задачами самостоятельной работы студентов являются:

· систематизация и закрепление полученных теоретических знаний и практических умений студентов;

· углубление и расширение теоретических знаний;

· формирование умения использовать справочную литературу;

· развитие познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности;

· формирование самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;

· развитие исследовательских умений.

В учебном процессе высшего учебного заведения выделяют два вида самостоятельной работы: аудиторная и внеаудиторная.

Аудиторная самостоятельная работа по дисциплине выполняется на учебных занятиях под непосредственным руководством преподавателя и по его заданиям.

Внеаудиторная самостоятельная работа выполняется студентом по заданию преподавателя, но без его непосредственного участия.

Внеаудиторная самостоятельная работа может включает такие формы работы, как: индивидуальные занятия (домашние занятия); изучение программного материала дисциплины (работа с учебником и конспектом лекции); изучение рекомендуемых литературных источников; конспектирование источников; выполнение контрольных работ; работа со словарями и справочниками; работа с электронными образовательными ресурсами и ресурсами Internet; выполнение типовых расчетов; подготовка презентаций; ответы на контрольные вопросы; подготовка докладов, рефератов; работа с компьютерными программами (математическими пакетами); подготовка к зачету, экзамену; групповая самостоятельная работа студентов; получение консультаций для разъяснений по вопросам изучаемой дисциплины.

Содержание самостоятельной работы студентов по изучению дисциплины «Математические основы защиты информации» представлено в таблице 4.

Таблица 4.

Содержание самостоятельной работы обучающихся

Номер радела (темы)	Темы/вопросы, выносимые на самостоятельное изучение	Кол-во часов	Формы работы
Матрицы и системы линейных алгебраических	Свойства матриц. Элементарные преобразования. Эквивалентные матрицы. Ступенчатые матрицы.	30	Самостоятельное изучение теоретического материала и методов решения типовых задач по данной теме.

уравнений			
Векторная алгебра	Свойства линейных операций. Замена базиса и системы координат.	30	Самостоятельное изучение теоретического материала и методов решения типовых задач по данной теме.
Прямая и плоскость	Угол между прямыми на плоскости. Расстояние от точки до плоскости. Условия параллельности и перпендикулярности.	15	Самостоятельное изучение теоретического материала и методов решения типовых задач по данной теме.
Линии и поверхности второго порядка	Квадратичные формы. Приведение квадратичных форм к каноническому виду.	15	Самостоятельное изучение теоретического материала и методов решения типовых задач по данной теме.
Целые числа и основы теории делимости	Доказательство теоремы об остатках. Расширенный алгоритм Евклида. Взаимообратные числа. Конечные цепные дроби. Диафантовы уравнения первой степени.	39	Самостоятельное изучение теоретического материала и методов решения типовых задач по данной теме.
Основы теории сравнений	Свойства сравнения. Виды полной системы вычетов. Исследование сравнений первой степени. Критерий разрешимости.	39	Самостоятельное изучение теоретического материала и методов решения типовых задач по данной теме.
Алгебраические структуры	Аддитивная группа. Мультипликативная группа. Смежные классы. Поле комплексных чисел.	39	Самостоятельное изучение теоретического материала и методов решения типовых задач по данной теме.
Многочлены	Степень многочлена. Деление с остатком. Теорема о делении с остатком. Алгоритм Евклида для многочленов. Тривиальные делители многочлена. Каноническое представление многочленов.	45	Самостоятельное изучение теоретического материала и методов решения типовых задач по данной теме.

5.3. Виды и формы письменных работ, предусмотренных при освоении дисциплины, выполняемые обучающимися самостоятельно.

В процессе изучения дисциплины «Математические основы защиты информации» предусмотрены следующие виды и формы письменных работ для самостоятельного выполнения:

1) аудиторная контрольная работа;
2) типовой расчет – внеаудиторная работа;
3) домашнее задание, как теоретического, так и практического характера;
4) экзаменационная работа.

Контрольные работы и экзаменационная работа выполняется студентом в аудитории. Типовой расчет выполняется вне аудитории за определенный промежуток времени, установленный преподавателем, оформляется в отдельной тетради. В установленный срок студент сдает типовой расчет и устно отчитывается преподавателю по выполненной работе.

6. ОБРАЗОВАТЕЛЬНЫЕ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

При реализации различных видов учебной работы по дисциплине могут использоваться электронное обучение и дистанционные образовательные технологии.

6.1. Образовательные технологии

Учебные занятия по дисциплине могут проводиться с применением информационно-

телекоммуникационных сетей при опосредованном (на расстоянии) интерактивном взаимодействии обучающихся и преподавателя в режимах on-line в формах: видеолекций, лекций-презентаций, видеоконференции, собеседования в режиме чат, форума, чата, выполнения виртуальных практических и/или лабораторных работ и др.

Максимальный объем занятий обучающегося с применением электронных образовательных технологий не должен превышать 25%.

Название образовательной технологии	Темы, разделы дисциплины	Краткое описание применяемой технологии
Типовые расчеты	Разделы 1, 2, 4, 5, 7	Проведение входного, текущего и рейтингового контроля знаний учащихся (в системах дистанционного обучения)
Консультации по электронной почте	Разделы 3, 6, 8	Подготовка к контрольным работам, выполнение типового расчета
Активная лекция	3. Основы теории сравнений	Лекция-визуализация
Активная лекция	8. Линии и поверхности второго порядка.	Лекция-визуализация

6.2. Информационные технологии

При реализации различных видов учебной и внеучебной работы используются следующие информационные технологии: виртуальная обучающая среда (или система управления обучением LMS Moodle) или иные информационные системы, сервисы и мессенджеры.

- использование электронных учебников и различных сайтов (например, электронные библиотеки, журналы и т.д.) как источник информации;
- использование возможностей электронной почты преподавателя для получения консультаций и обмена учебной информацией;
- использование средств представления учебной информации (лекции с использованием презентаций);
- использование математических пакетов и офисных программ.

6.3. Перечень программного обеспечения и информационных справочных систем

а) Перечень лицензионного учебного программного обеспечения.

Наименование программного обеспечения	Назначение
Adobe Reader	Программа для просмотра электронных документов
Платформа дистанционного обучения LMS Moodle	Виртуальная обучающая среда
Mozilla FireFox	Браузер
Microsoft Office 2013	Офисная программа
7-zip	Архиватор
Microsoft Windows 7 Professional	Операционная система
Kaspersky Endpoint Security	Средство антивирусной защиты
Microsoft Visual Studio	Среда разработки

б) Информационные справочные системы:

1. Электронный каталог Научной библиотеки АГУ на базе MARK SQL НПО «Информ-систем»: https://library.asu.edu.ru.
2. Электронный каталог «Научные журналы АГУ»: http://journal.asu.edu.ru/.
3. Универсальная справочно-информационная полнотекстовая база данных периодических изданий ООО «ИВИС»: http://dlib.eastview.com/
4. Электронно-библиотечная система elibrary. http://elibrary.ru
5. Справочная правовая система КонсультантПлюс: http://www.consultant.ru
6. Информационно-правовое обеспечение «Система ГАРАНТ»: http://garant-astrakhan.ru

7. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

7.1. Паспорт фонда оценочных средств

При проведении текущего контроля и промежуточной аттестации по дисциплине «Математические основы защиты информации» проверяется сформированность у обучающихся компетенций, указанных в разделе 3 настоящей программы. Этапность формирования данных компетенций в процессе освоения образовательной программы определяется последовательным освоением дисциплин (модулей) и прохождением практик, а в процессе освоения дисциплины – последовательным достижением результатов освоения содержательно связанных между собой разделов, тем.

Таблица 5
Соответствие разделов, тем дисциплины (модуля), результатов обучения по дисциплине (модулю) и оценочных средств

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
1.	Матрицы и системы линейных алгебраических уравнений	ОПК-3, ОПК-11, ОПК-12	Типовой расчет 1 «Матрицы и системы линейных алгебраических уравнений». Опрос на экзамене
2.	Векторная алгебра	ОПК-3, ОПК-11, ОПК-12	Типовой расчет 2 «Векторная алгебра». Опрос на экзамене
3.	Прямая и плоскость	ОПК-3, ОПК-11, ОПК-12	Контрольная работа 1 «Прямая и плоскость». Опрос на экзамене
4.	Линии и поверхности второго порядка	ОПК-3, ОПК-11, ОПК-12	Типовой расчет 3 «Линии и поверхности второго порядка». Опрос на экзамене
5.	Целые числа и основы теории делимости	ОПК-3, ОПК-11, ОПК-12	Типовой расчет 4 «Целые числа и основы теории делимости». Лабораторная работа 1 «Алгоритм Евклида». Лабораторная работа 2 «Простые числа». Опрос на экзамене
6.	Основы теории сравнений	ОПК-3, ОПК-11, ОПК-12	Контрольная работа 2 «Основы теории сравнений». Опрос на экзамене
7.	Алгебраические структуры	ОПК-3, ОПК-11, ОПК-12	Типовой расчет 5 «Алгебраические структуры». Опрос на экзамене
8.	Многочлены	ОПК-3, ОПК-11, ОПК-12	Контрольная работа 3 «Многочлены». Опрос на экзамене

7.2. Описание показателей и критериев оценивания компетенций, описание шкал оценивания

Таблица 6

Показатели оценивания результатов обучения в виде знаний

Шкала оценивания	Критерии оценивания
5 «отлично»	демонстрирует глубокое знание теоретического материала, умение обоснованно излагать свои мысли по обсуждаемым вопросам, способность полно, правильно и аргументированно отвечать на вопросы, приводить примеры
4 «хорошо»	демонстрирует знание теоретического материала, его последовательное изложение, способность приводить примеры, допускает единичные ошибки, исправляемые после замечания преподавателя
3 «удовлетвори тельно»	демонстрирует неполное, фрагментарное знание теоретического материала, требующее наводящих вопросов преподавателя, допускает существенные ошибки в его изложении, затрудняется в приведении примеров и формулировке выводов
2 «неудовлетво рительно»	демонстрирует существенные пробелы в знании теоретического материала, не способен его изложить и ответить на наводящие вопросы преподавателя, не может привести примеры

Таблица 7

Показатели оценивания результатов обучения в виде умений и владений

Шкала оценивания	Критерии оценивания
5 «отлично»	демонстрирует способность применять знание теоретического материала при выполнении заданий, последовательно и правильно выполняет задания, умеет обоснованно излагать свои мысли и делать необходимые выводы
4 «хорошо»	демонстрирует способность применять знание теоретического материала при выполнении заданий, последовательно и правильно выполняет задания, умеет обоснованно излагать свои мысли и делать необходимые выводы, допускает единичные ошибки, исправляемые после замечания преподавателя
3 «удовлетвори тельно»	демонстрирует отдельные, несистематизированные навыки, не способен применить знание теоретического материала при выполнении заданий, испытывает затруднения и допускает ошибки при выполнении заданий, выполняет задание при подсказке преподавателя, затрудняется в формулировке выводов
2 «неудовлетво рительно»	не способен правильно выполнить задание

7.3. Контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности

СЕМЕСТР 2

Тема «Матрицы и системы линейных алгебраических уравнений»

1. ***Типовой расчет «Матрицы и системы линейных алгебраических уравнений».***

Инструкция по выполнению типового расчета.

Внимательно прочитайте задания. При выполнении заданий можно использовать конспекты лекций, рабочую тетрадь, справочную литературу. Задания выполняются в отдельной тетради, на которой необходимо записать Ф.И.О. студента, группу, номер варианта, в каждом задании записывается номер задания, условие задания, подробное решение, ответ. Выполненные задания необходимо сдать преподавателю в установленный срок и затем отчитаться преподавателю по типовому расчету. За нарушение сроков сдачи типового расчета оценка снижается.

Вариант 0

Задание 1. Для данного определителя найти миноры и алгебраические дополнения элементов a_{i2}, a_{3j}. Вычислить определитель: а) разложив его по элементам *i*-й строки; б) разложив его по элементам *j*-го столбца; в) получив предварительно нули в i-й строке.

$$\begin{vmatrix} -3 & 2 & 1 & 0 \\ 2 & -2 & 1 & 4 \\ 4 & 0 & -1 & 2 \\ 3 & 1 & -1 & 4 \end{vmatrix}.$$

Задание 2. Даны две матрицы А и В. Найти: а) АВ; б) ВА; в) А-1; г) AA^{-1}

$$A = \begin{pmatrix} -4 & 0 & 1 \\ 2 & -1 & 3 \\ 3 & 2 & 4 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 2 & -3 \\ 2 & 0 & 1 \\ -2 & 1 & 3 \end{pmatrix}.$$

Задание 3. Проверить совместимость системы уравнений и в случае совместимости решить ее.

$$\begin{cases} 3x - 2y - 3z = 0 \\ x + 5y + 3z = 1 \\ 2x - 3y - 4z = 3 \end{cases}$$

Тема «Векторная алгебра».

1. ***Типовой расчет «Векторная алгебра»***

Инструкция по выполнению типового расчета.

Внимательно прочитайте задания. При выполнении заданий можно использовать конспекты лекций, рабочую тетрадь, справочную литературу. Задания выполняются в отдельной тетради, на которой необходимо записать Ф.И.О. студента, группу, номер вариант. Можно использовать тетрадь с типовым расчетом 1. В каждом задании записывается номер задания, условие задания, подробное решение, ответ. Выполненные задания необходимо сдать преподавателю в установленный срок и затем отчитаться преподавателю по типовому расчету. За нарушение сроков сдачи типового расчета оценка снижается.

Вариант 0.

Задание 1: Коллинеарны ли векторы $\vec{c}_1$ и $\vec{c}_2$, разложенные по векторам $\vec{a}$ и $\vec{b}$, где $\vec{c}_1 = 5\vec{a} + 3\vec{b}, \vec{c}_2 = 4\vec{a} + \vec{b}, \vec{a} = \{2;-1;5\}, \vec{b} = \{7;1;-3\}$.

Задание 2: Перпендикулярны ли векторы $\vec{a} = \{-7;1;2\}, \vec{b} = \{3;2;-1\}$?

Задание 3: Компланарны ли векторы $\vec{a} = \{-1;2;-1\}, \vec{b} = \{0;2;1\}, \vec{c} = \{2;0;3\}$?

Задание 4: При каком значении α векторы $\vec{AB}, \vec{AC}$, где $A(2;1;\alpha), B(3;1;4), C(2;5;3).$, перпендикулярны?

Задание 5: Даны точки: $A(1;0;-1), B(0;1;3), C(2;0;1)$.

Найти:

a) $\text{пр}_{(\vec{AB}+\vec{CB})}\left(2\vec{AC}+3\vec{CB}\right)$;

b) $\left|\vec{AB}+4\vec{BC}\right|$;

c) $\angle\left(\vec{AB}-\vec{CB},\vec{AB}\right)$;

d) орт вектора $\vec{AB}$;

e) $\left(\left(\vec{AB}+4\vec{BC}\right),\left(\vec{BA}-\vec{AC}\right)\right)$;

f) $\left[\left(\vec{AB}+2\vec{BC}\right),\left(\vec{CB}-\vec{AB}\right)\right]$;

g) $\vec{AB}\cdot\vec{BC}\cdot\vec{AC}$;

Задание 6: Даны координаты вершин пирамиды: $A(1;4;3), B(2;3;1), C(-2;1;3), D(0;1;2)$.

Вычислить:

a) объем пирамиды;
b) длину ребра AB;
c) площадь грани ABC;

Тема «Прямая и плоскость»

1. Контрольная работа «Прямая и плоскость»

Инструкция по выполнению контрольной работы.
Внимательно прочитайте задания. При выполнении заданий нельзя пользоваться интернетом, можно использовать конспекты лекций, рабочую тетрадь, справочную литературу. Задания выполняются на отдельном листе, на котором необходимо записать Ф.И.О. студента, группу, номер варианта, в каждом задании записывается номер задания, условие задания, подробное решение, ответ. Время выполнения контрольной работы – 90 минут. При невыполнении инструкции студент получает неудовлетворительную оценку.

Вариант 0.

1. Даны координаты вершин треугольника АВС. А(−1; 5), В(3; 1) и С(1; -2). Требуется написать уравнения:
   a. стороны ВС ;
   b. высоты, опущенной из вершины А на сторону ВС;
   c. медианы, проведенной из вершины С.
   d. Найти периметр и площадь треугольника АВС.
2. Определить расстояние от точки М до прямой 20x – 21 y – 58 = 0.
3. Написать каноническое уравнение прямой $\begin{cases} 2x+3y-2z+6=0 \\ x-3y+z+3=0 \end{cases}$
4. Найти угол между плоскостями x + 2y - 2z – 7 = 0 и x + y - 35 = 0.
5. Доказать, что прямая $\frac{x-1}{2}=\frac{y+2}{3}=\frac{z-1}{6}$ перпендикулярна к прямой $\begin{cases} 2x+y-4z+2=0 \\ 4x-y-5z+4=0 \end{cases}$.
6. Даны четыре точки: А(3, -1, 2), В(-1, 0, 1), С(1, 7, 3), Д(8, 5, 8). Найти:

а. уравнение плоскости АВС;
б. уравнение и длину высоты пирамиды АВСД, проведенной из точки Д;
в. уравнение и длину ребра АС.

Тема «Линии и поверхности второго порядка»

1. ***Типовой расчет «Линии и поверхности второго порядка»***

Инструкция по выполнению типового расчета.
Внимательно прочитайте задания. При выполнении заданий можно использовать конспекты лекций, рабочую тетрадь, справочную литературу. Задания выполняются в отдельной тетради, на которой необходимо записать Ф.И.О. студента, группу, номер варианта. Можно использовать тетрадь с предыдущими типовыми расчетами. В каждом задании записывается номер задания, условие задания, подробное решение, ответ. Выполненные задания необходимо сдать преподавателю в установленный срок и затем отчитаться преподавателю по типовому расчету. За нарушение сроков сдачи типового расчета оценка снижается.

Вариант 0

Задание 1. Выполнив последовательно преобразования координат: поворот, а затем параллельный перенос координатных осей, преобразовать к каноническому виду уравнение кривой второго порядка и построить ее в канонической и исходной системе координат, а также найти параметры кривой.

$$5x^2 + 5y^2 + 6xy - 8\sqrt{2}x - 8\sqrt{2}y = 0$$

Задание 2. Приведенные поверхности ограничивают в пространстве некоторые тела вращения конечных размеров. Назвать типы этих поверхностей и нарисовать тело в данной системе координат.

$$a)\ z = \sqrt{4 - x^2 - y^2}, \quad z = \sqrt{x^2 + y^2} - 2;$$

$$b)\ y = x^2 + z^2, \quad y = 4;$$

$$c)\ z = 1 + \sqrt{2} - \sqrt{4 - x^2 - y^2}, \quad z = -1 + x^2 + y^2,$$
$$z = -1 + \sqrt{x^2 + y^2}.$$

Экзамен

Экзаменационный билет включает в себя 1 теоретический вопрос и 2 задачи. Список теоретических вопросов представлен ниже. Формулировки задач аналогичны задачам, которые решилась в течение семестра.

Инструкция по выполнению экзаменационной работы.
Внимательно прочитайте задания. При выполнении заданий нельзя пользоваться интернетом, конспектами лекций, рабочей тетрадью, справочной литературой. Задания выполняются на отдельном листе, на котором необходимо записать Ф.И.О. студента, группу, номер билета, в каждом задании записывается номер задания, условие задания, подробное решение, ответ. Время выполнения экзаменационной работы – 40 минут.
При невыполнении инструкции студент получает неудовлетворительную оценку.

Билет №0

Задание № 1. Теоретический вопрос (смотри список вопросов к экзамену).
Задание № 2. Решить систему уравнений методом обратной матрицы. Сделать проверку.

$$\begin{cases} 2x + y - z = 5 \\ 3x + 3y - 2z = 8. \\ x + y + z = 6 \end{cases}$$

Задание №3. Даны точки А(–5;2), В(5;7), С(3;- 3). Составить общее уравнение прямой, проходящей через точку С параллельно прямой АВ. Составить общее уравнение прямой, проходящей через точку С перпендикулярно прямой АВ.

Контрольные вопросы к экзамену (1ый семестр)

1. Матрицы, определители матриц. Свойства определителя.
2. Миноры и алгебраические дополнения. Дополнительные свойства определителя квадратной матрицы.
3. Обратные матрицы.
4. Элементарные преобразования матриц. Эквивалентные матрицы.
5. Ранг матрицы.
6. Системы линейных уравнений. Равносильность систем уравнений. Теорема Крамера.
7. Системы линейных уравнений. Метод Гаусса.
8. Система линейных однородных уравнений. Фундаментальный набор решений однородной системы линейных уравнений.
9. Геометрические векторы и линейные операции над ними.
10. Коллинеарные векторы. Компланарные векторы. Теорема о компланарных векторах.
11. Базис векторного пространства. Координаты вектора в заданном базисе. Сложение векторов и умножение вектора на число в координатах. Признак коллинеарности двух векторов в координатах. Признак компланарности трех векторов в координатах.
12. Системы координат. Декартова система координат. Координаты точки в пространстве. Решение двух основных задач в декартовой системе координат.
13. Системы координат. Декартова прямоугольная система координат. Полярная система координат. Связь между полярными и прямоугольными координатами точки плоскости.
14. Замена базиса и системы координат. Формулы перехода от одной системы координат к другой. Формулы переноса начала координат.
15. Скалярное произведение векторов. Теорема о скалярном произведении векторов в координатной форме. Свойства скалярного произведения.
16. Векторное произведение двух векторов и его свойства. Формула векторного произведения в координатах.
17. Смешанное произведение трех векторов, его геометрический смысл и свойства. Формула смешанного произведения в координатах.
18. Линия первого порядка. Уравнения прямой на плоскости.
19. Линии второго порядка: эллипс, гипербола, парабола.
20. Плоскость как поверхность первого порядка. Уравнения плоскости.
21. Уравнения прямой в пространстве.
22. Поверхности второго порядка.
23. Определение, свойства векторного пространства. Конечномерные векторные пространства.
24. Линейные преобразования векторных пространств. Собственные векторы и собственные значения линейного преобразования.

СЕМЕСТР 3

Тема «Целые числа и основы теории делимости».

1. Типовой расчет «Целые числа и основы теории делимости»

Инструкция по выполнению типового расчета.

Внимательно прочитайте задания. При выполнении заданий можно использовать конспекты лекций, рабочую тетрадь, справочную литературу. Задания выполняются в отдельной тетради, на которой необходимо записать Ф.И.О. студента, группу, номер варианта, в каждом задании записывается номер задания, условие задания, подробное решение, ответ. Выполненные задания необходимо сдать преподавателю в установленный срок и затем отчитаться преподавателю по типовому расчету. За нарушение сроков сдачи типового расчета оценка снижается.

Вариант 0

Задание 1. Найдите НОД двух чисел a = 2552, b = 826, c = 106.

Задание 2. Записать НОД чисел a и b в линейной форме. a = 496, b = 204.

Задание 3. Найдите НОК чисел a = 1812, b = 592

Задание 4. Найдите все простые числа, заключенные между a и b. a = 1416, b = 1436.

Задание 5. Найти каноническое разложение числа a = 2494800.

Задание 6. Записать число a/b в виде непрерывной дроби. a = 1377, b = 122.

Задание 7. Непрерывную дробь $[q_1, q_2, q_3, q_4]$ записать в виде a/b. $q_1 = 15$, $q_2 = 7$, $q_3 = 16$, $q_4 = 2$.

Задание 8. С помощью разложения в непрерывную дробь сократить дробь a/b. a = 14223, b = 2016.

2. ***Лабораторная работа «Алгоритм Евклида»***

Написать программу на языке высокого уровня для реализации решения каждого из заданий. Предусмотреть формирование чисел *a,b,c* программно и ввод чисел с клавиатуры.

Задание №1. Найти *НОД* трех целых чисел:

- с помощью вспомогательной программы отыскания *НОД* двух целых чисел;
- с помощью реализации алгоритма Евклида для трех чисел одновременно.

Задание №2. Найти линейное представление *НОД(a,b)*.

Задание №3. Найти *НОК* трех целых чисел.

3. ***Лабораторная работа «Простые числа»***

Написать программу на языке высокого уровня для реализации решения каждого из заданий.

Задание №1. Напишите вспомогательную программу построения таблицы простых чисел меньших 256 с помощью решета Эратосфена.

Задание №2. Выясните с помощью метода Ферма, являются ли n произвольных чисел простыми; в случае составного числа разложите его на множители.

Задание №3. Для произвольного большого простого числа p выясните вопрос о его простоте:

- с помощью теста Соловея – Штрассена;
- с помощью теста Лемана;
- с помощью теста Рабина – Миллера;
- с помощью непосредственной проверки.

Тема «Основы теории сравнений»

1. ***Контрольная работа «Основы теории сравнений».***

Инструкция по выполнению контрольной работы.
Внимательно прочитайте задания. При выполнении заданий нельзя пользоваться интернетом, можно использовать конспекты лекций, рабочую тетрадь, справочную литературу. Задания выполняются на отдельном листе, на котором необходимо записать Ф.И.О. студента, группу, номер варианта, в каждом задании записывается номер задания, условие задания, подробное решение, ответ. Время выполнения контрольной работы – 90 минут. При невыполнении инструкции студент получает неудовлетворительную оценку.

Вариант 0.

Задание 1. Решите диофантово уравнение 275x + 145y = 15.

Задание 2. Найдите остаток от деления числа $*36^{13*}$ на 2*, где * – номер варианта.

Задание 3. Решите сравнение первой степени $442x \equiv 22\ (mod\ 646)$.

Задание 4. Решите систему сравнений первой степени

$$\begin{cases} x \equiv 12(mod\ 19) \\ 2x \equiv 5(mod\ 21) \\ x \equiv 8(mod\ 23) \end{cases}$$

Тема «Алгебраические структуры»

1. ***Типовой расчет «Алгебраические структуры».***

Инструкция по выполнению типового расчета.
Внимательно прочитайте задания. При выполнении заданий можно использовать конспекты лекций, рабочую тетрадь, справочную литературу. Задания выполняются в отдельной тетради, на которой необходимо записать Ф.И.О. студента, группу, номер варианта, в каждом задании записывается номер задания, условие задания, подробное решение, ответ. Выполненные задания необходимо сдать преподавателю в установленный срок и затем отчитаться преподавателю по типовому расчету. За нарушение сроков сдачи типового расчета оценка снижается.

Вариант 0

1. Является ли операция f алгебраической на множестве $A = \{x \mid x \in \boldsymbol{R}, x > 0\}$. Если да, проверьте свойства коммутативности, ассоциативности?
   $afb = \frac{a+b}{2}$,
2. Является ли множество А относительно указанной операции f группой.
   $A = \{x \mid x = 2^n,\ n \in Z\}$, f – обычное умножение.
3. Построить кольцо Z_{10}. Указать в нем:
   a. для каждого элемента противоположный элемент;
   b. указать все обратимые элементы и для каждого из них обратный элемент;

c. показать, что все обратимые элементы в данном кольце мультипликативную группу;
d. является ли кольцо полем;
e. в каждом из указанных колец указать делители нуля.

4. Решить систему линейных уравнений:

$$\begin{cases} 2x + 3y = 1 \\ 2x - y = 2 \end{cases} \text{ в } Z_5$$

Тема «Многочлены»

1. Контрольная работа «Многочлены».

Инструкция по выполнению контрольной работы.
Внимательно прочитайте задания. При выполнении заданий нельзя пользоваться интернетом, можно использовать конспекты лекций, рабочую тетрадь, справочную литературу. Задания выполняются на отдельном листе, на котором необходимо записать Ф.И.О. студента, группу, номер варианта, в каждом задании записывается номер задания, условие задания, подробное решение, ответ. Время выполнения контрольной работы – 60 минут. При невыполнении инструкции студент получает неудовлетворительную оценку.

Вариант 0.

1. Найти остаток от деления многочлена $2x^6 – x^5 + 12x^3 - 72x^2 + 3$ на многочлен $x^3 + 2x^2 – 1$.
2. Найдите НОД и НОК многочленов $x^6 − 4x^5 + 2x^4 + 5x^3 + 2x^2 − 4x − 8$ и $x^5 − x^4 − x^3 + x^2 − 4x − 4$.
3. Проверьте, что 2 является корнем многочлена: $p(x) = 2x^7 + x^6 − 12x^5 − 14x^4 + 14x^3 + 33x^2 + 20x + 4$. Найдите остальные корни этого многочлена.
4. Разложите многочлен $4x^3 + 8x^2 – x$ на множители.

Экзамен

Экзаменационный билет включает в себя 1 теоретический вопрос и 2 задачи. Список теоретических вопросов представлен ниже. Формулировки задач аналогичны задачам, которые решилась в течение семестра.

Инструкция по выполнению экзаменационной работы.
Внимательно прочитайте задания. При выполнении заданий нельзя пользоваться интернетом, конспектами лекций, рабочей тетрадью, справочной литературой. Задания выполняются на отдельном листе, на котором необходимо записать Ф.И.О. студента, группу, номер билета, в каждом задании записывается номер задания, условие задания, подробное решение, ответ. Время выполнения экзаменационной работы – 40 минут.
При невыполнении инструкции студент получает неудовлетворительную оценку.

Билет №0

Задание № 1. Теоретический вопрос (смотри список вопросов к экзамену).

Задание №2. Найти НОД и НОК чисел: 126, 249, 673.

Задание №3. Решите сравнение первой степени $58x \equiv 87\ (mod\ 47)$.

Контрольные вопросы к экзамену (2ой семестр)

1. Отношение делимости и его простейшие свойства. Теорема о делении с остатком.
2. НОД. Свойства НОД. Алгоритм Евклида.
3. Взаимно простые числа и их свойства. НОК и его свойства.

4. Простые числа. Критерий простоты числа. Решето Эратосфена.
5. Разложение целых чисел на простые множители. Основная теорема арифметики.
6. Конечные цепные дроби. Подходящие дроби данной цепной дроби.
7. Неопределенные (диофантовы) уравнения I степени с двумя переменными.
8. Определение и простейшие свойства сравнений.
9. Полная и приведенная система вычетов. Теорема 1 о вычетах. Теорема 2 о вычетах.
10. Теоремы Эйлера и Ферма.
11. Сравнения с неизвестной величиной. Исследование и решение сравнений первой степени.
12. Методы решений сравнений первой степени.
13. Системы сравнений первой степени с одним неизвестным.
14. Алгебраические (бинарные) операции на множестве. Группа. Примеры групп. Конечные абелевы группы.
15. Подгруппы. Разложение группы в смежные классы. Теорема Лагранжа.
16. Нормальные делители группы. Факторгруппа.
17. Циклические группы.
18. Кольца. Примеры колец. Подкольцо. Кольцо вычетов. Кольцо с делителями нуля.
19. Поле. Примеры полей. Подполе.
20. Поле комплексных чисел.
21. Матрицы над кольцом и операции над ними.
22. Определители матриц над коммутативным кольцом с единицей. Свойства определителя.
23. Миноры и алгебраические дополнения элементов матрицы. Дополнительные свойства определителя квадратной матрицы.
24. Обратимые матрицы над кольцом. Критерий обратимости.
25. Элементарные преобразования матриц. Эквивалентные матрицы.
26. Матрицы над полем. Ранг матрицы.
27. Системы линейных уравнений над коммутативным кольцом с единицей. Равносильность систем уравнений. Теорема Крамера.
28. Системы линейных уравнений над полем. Метод Гаусса.
29. Система линейных однородных уравнений. Фундаментальный набор решений однородной системы линейных уравнений.
30. Кольцо многочленов от одной переменной над кольцом К. Степень многочлена.
31. Делимость многочленов над полем. Теорема о делении многочлена с остатком.
32. НОД многочленов, его свойства. Алгоритм Евклида для нахождения НОД многочленов. НОК многочленов.
33. Неприводимые над полем многочлены. Разложение многочлена на неприводимые множители.
34. Корни многочлена. Теорема Безу. Поле разложения многочлена.

7.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

По дисциплине «Математические основы защиты информации» итоговой формой отчетности в первом и втором семестрах является экзамен. Согласно действующей в АГУ системе оценивания БАРС для дисциплин, итоговой формой отчетности для которых является экзамен, отводится 100 баллов, которые складываются из двух частей: семестровой оценки (текущий контроль по учебной дисциплине в течение семестра) – 50 баллов и экзаменационной – 50 баллов. 50 баллов семестрового контроля состоят из 40 баллов полученных на различных формах текущего контроля и 10 баллов, включающих различного рода бонусы. Система накопления баллов, а также система штрафов, представлена в технологических картах дисциплины «Математические основы защиты информации».

ТЕХНОЛОГИЧЕСКАЯ КАРТА (семестр 1)

Итоговый контроль (экзамен): экзамен – 50 баллов.
Максимальное количество баллов по формам контроля:

- Типовой расчет 1 «Матрицы и системы линейных алгебраических уравнений» – 15 баллов.
- Типовой расчет 2 «Векторная алгебра» – 14 баллов.
- Контрольная работа 1 «Прямая и плоскость» – 6 баллов.
- Типовой расчет 3 «Линии и поверхности второго порядка» – 5 баллов.

Бонусные баллы:

- Посещение занятий – 0,1 балл за занятие, но не более 2 баллов
- Активность студента на занятии – 0,3 балла за занятие, но не более 6 баллов
- Аккуратное оформление конспектов лекций – 2 балла

ТЕХНОЛОГИЧЕСКАЯ КАРТА (семестр 2)

Итоговый контроль (экзамен): экзамен – 50 баллов.
Максимальное количество баллов по формам контроля:

- Типовой расчет 4 «Целые числа и основы теории делимости» - 8 баллов.
- Лабораторная работа 1 «Алгоритм Евклида» - 6 баллов (по 2 балла за каждое задание).
- Лабораторная работа 2 «Простые числа» - 6 баллов (по 2 балла за каждое задание)
- Контрольная работа 2 «Основы теории сравнений» - 6 баллов.
- Типовой расчет 5 «Алгебраические структуры» - 10 баллов.
- Контрольная работа 3 «Многочлены» - 4 балла.

Бонусные баллы:

- Посещение занятий – 0,1 балл за занятие, но не более 2 баллов
- Активность студента на занятии – 0,3 балла за занятие, но не более 6 баллов
- Аккуратное оформление конспектов лекций – 2 балла

По каждому контрольному мероприятию предусмотрен обязательный минимум усвоения материала, предусмотренного учебной программой (60% от максимального количества баллов), который должен быть достигнут каждым студентом для аттестации по дисциплине «Математические основы защиты информации».

Преподаватель, реализующий дисциплину, в зависимости от уровня подготовленности, обучающихся может использовать иные формы, методы контроля и оценочные средства, исходя из конкретной ситуации.

8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

а) Основная литература:

1. Основы математической обработки информации / М.С. Мирзоев - М. : Прометей, 2016. – URL: http://www.studentlibrary.ru/book/ISBN9785906879011.html (ЭБС «Консультант студента»)
2. Краткий курс высшей алгебры и аналитической геометрии: учебник / Дураков Б.К. - Красноярск : СФУ, 2017. - http://www.studentlibrary.ru/book/ISBN9785763837360.html (ЭБС «Консультант студента»)
3. Краткий курс алгебры и геометрии. Примеры, задачи, тесты : учебное пособие / Н.В. Никонова, Н.Н. Газизова, Г.А. Никонова. - Казань : Издательство КНИТУ, 2014. -

http://www.studentlibrary.ru/book/ISBN9785788217116.html (ЭБС «Консультант студента»)
4. Специальные главы высшей математики: учебно-методическое пособие / Кучер Е.С. - Новосибирск : Изд-во НГТУ, 2017. - http://www.studentlibrary.ru/book/ISBN9785778231542.html (ЭБС «Консультант студента»)
5. Высшая математика. Линейная алгебра и аналитическая геометрия / Геворкян П.С - М. : ФИЗМАТЛИТ, 2014. - http://www.studentlibrary.ru/book/ISBN9785922115827.html (ЭБС «Консультант студента»)
6. Аверченков В.И., Служба защиты информации : организация и управление [Электронный ресурс] / В.И. Аверченков, М.Ю. Рытов - М. : ФЛИНТА, 2016. - 186 с. - ISBN 978-5-9765-1271-9 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785976512719.html ЭБС «Консультант студента»
7. Милославская Н.Г., Технические, организационные и кадровые аспекты управления информационной безопасностью [Электронный ресурс] : Учебное пособие для вузов / Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. - Вып. 4. - М. : Горячая линия - Телеком, 2013. - 216 с. (Серия "Вопросы управления информационной безопасностью") - ISBN 978-5-9912-0274-9 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991202749.html ЭБС «Консультант студента»
8. Аверченков В.И., Защита персональных данных в организации [Электронный ресурс] / В.И. Аверченков, М.Ю. Рытов, Т.Р. Гайнулин - М. : ФЛИНТА, 2016. - 124 с. - ISBN 978-5-9765-1273-3 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785976512733.html ЭБС «Консультант студента»
9. Аверченков В.И., Криптографические методы защиты информации [Электронный ресурс] / Аверченков В.И. - М. : ФЛИНТА, 2017. - 215 с. - ISBN 978-5-9765-2947-2 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785976529472.html ЭБС «Консультант студента»

б) Дополнительная литература:

1. Математические методы в теории защиты информации / Горбунов В.А. - М: Издательство Московского государственного горного университета, 2004. - URL: http://www.studentlibrary.ru/book/ISBN5741803393.html (ЭБС «Консультант студента»)
2. Высшая математика в примерах и задачах] : учебное пособие для вузов. В 3 т.: Т. 2 / В.Д. Черненко. - 2-е изд., перераб. и доп. - СПб. : Политехника, 2011. - URL: http://www.studentlibrary.ru/book/ISBN97857325098612.html (ЭБС «Консультант студента»)
3. Линейная алгебра и геометрия. / Шафаревич И.Р., Ремизов А.О. - М. : ФИЗМАТЛИТ, 2009. - URL: http://www.studentlibrary.ru/book/ISBN9785922111393.html (ЭБС «Консультант студента»)
4. Демидович, Б.П. Основы вычислительной математики : учеб. пособие / Б. П. Демидович, И. А. Марон. - 8-е изд. ; стер. - СПб.; М.; Краснодар : Лань, 2011. - 672 с. - (Учеб. для вузов. Спец. лит.). - ISBN 978-5-8114-0695-1 : 850-08.
5. Кузнецов, А.В. Высшая математика. Математическое программирование : учеб. / А. В. Кузнецов, Сакович, В.А., Холод, Н.И. ; под общ. ред. А.В. Кузнецова. - Изд. 3-е ; стер. - СПб. : Лань, 2010. - 352 с. : ил. - (Учебники для вузов. Специальная литература). - ISBN 978-5-8114-1056-9 : 350-02.
6. Сборник задач и упражнений по высшей математике. Математическое программирование : учеб. пособ. / под общ. ред. А.В. Кузнецова, Р.А. Рутковского. - Изд. 3-е ; стер. - СПб. : Лань, 2010. - 448 с. : ил. - (Учебники для вузов. Специальная литература). - ISBN 978-5-8114-1057-6 : 480-04.

7. Мальцев, И.А. Линейная алгебра : учеб. пособ. / И. А. Мальцев. - 2-е изд. ; испр. и доп. - СПб. : Лань, 2010. - 384 с. : ил. - (Учебники для вузов. Специальная литература). - ISBN 978-5-8114-1011-8 : 645-92.
8. Девянин П.Н., Модели безопасности компьютерных систем. Управление доступом и информационными потоками [Электронный ресурс] : Учебное пособие для вузов / Девянин П.Н. - 2-е изд., испр. и доп. - М. : Горячая линия - Телеком, 2013. - 338 с. - ISBN 978-5-9912-0328-9 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991203289.html ЭБС «Консультант студента»
9. Васильев В.И., Интеллектуальные системы защиты информации [Электронный ресурс] : учеб. пособие/ Васильев В.И. - 2-е изд., испр. и доп. - М.: Машиностроение, 2013. - 172 с. - ISBN 978-5-94275-667-3 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785942756673.html ЭБС «Консультант студента»
10. Волгин В.В., Погрузка и разгрузка [Электронный ресурс] / Волгин В. В. - М. : Дашков и К, 2014. - 592 с. - ISBN 978-5-394-01621-9 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785394016219.html ЭБС «Консультант студента»
11. Малюк А.А., Защита информации в информационном обществе [Электронный ресурс]: Учебное пособие для вузов. / А.А. Малюк - М. : Горячая линия - Телеком, 2015. - 230 с. - ISBN 978-5-9912-0481-1 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991204811.html ЭБС «Консультант студента»
12. Аверченков В.И., Системы защиты информации в ведущих зарубежных странах [Электронный ресурс] / В.И. Аверченков, М.Ю. Рытов, Г.В. Кондрашин, М.В. Рудановский - М. : ФЛИНТА, 2016. - 224 с. (Серия "Организация и технология защиты информации") - ISBN 978-5-9765-1274-0 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785976512740.html ЭБС «Консультант студента»

в) Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимый для освоения дисциплины (модуля)

1. **Электронно-библиотечная система (ЭБС) ООО «Политехресурс» «Консультант студента».** Многопрофильный образовательный ресурс «Консультант студента» является электронной библиотечной системой, предоставляющей доступ через сеть Интернет к учебной литературе и дополнительным материалам, приобретенным на основании прямых договоров с правообладателями. Каталог в настоящее время содержит около 15000 наименований. www.studentlibrary.ru.

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Для проведения лекционных занятий необходима мультимедийная аудитория, оснащенная компьютерной презентационной техникой.

При необходимости рабочая программа дисциплины (модуля) может быть адаптирована для обеспечения образовательного процесса инвалидов и лиц с ограниченными возможностями здоровья, в том числе для обучения с применением дистанционных образовательных технологий. Для этого требуется заявление студента (его законного представителя) и заключение психолого-медико-педагогической комиссии (ПМПК).