Министерство науки и высшего образования Российской Федерации

ФГБОУ ВО «Тверской государственный университет»

Утверждаю:

Руководитель ООП:

_____ Н.А. Семыкина

«9» 06 2023 г.

Рабочая программа дисциплины (с аннотацией)

Методы алгебраической геометрии в криптографии

Специальность

10.05.01 Компьютерная безопасность

Специализация

«Математические методы защиты информации»

Для студентов 5 курса очной формы обучения

Уровень высшего образования

СПЕЦИАЛИТЕТ

Составители:

ст. преподаватель С.А. Желтов.

Тверь 2023

I. Аннотация

1. Наименование дисциплины (модуля) в соответствии с учебным планом

Методы алгебраической геометрии в криптографии.

2. Цель и задачи дисциплины (модуля)

Целью освоения дисциплины (модуля) является:

формирование базы для развития профессиональных компетенций, связанных с готовностью студента к деятельности в области проектирования и построения криптографических протоколов на эллиптических кривых, предназначенных для решения различных профессиональных, исследовательских и прикладных задач.

Задачами освоения дисциплины (модуля) являются:

- получение базовых знаний и умений, связанных с основными понятиями алгебраической геометрии;
- получение теоретических знаний о роли и назначении различных криптосистем на базе эллиптических кривых;
- обучения студентов общим принципам и методам построения криптографических систем на основе эллиптических кривых;
- получение теоретических знаний и практических навыков о основных методах и алгоритмах дискретного логарифмирования на эллиптических кривых;

3. Место дисциплины (модуля) в структуре ООП

Дисциплина входит в вариативную часть ООП .

Для освоения дисциплины студент должен владеть современными методами и средствами информационных технологий. Необходимы знания, умения и компетенции, полученные студентами на занятиях по дисциплинам алгебра, криптографические методы защиты информации, теоретико-числовые методы в криптографии. Знания и практические навыки, полученные из курса, используются студентами при прохождении производственной и преддипломной практики, а также при разработке курсовых и дипломных работ.

4. Объем дисциплины (или модуля):

2 зачетных единиц, *72* академических часов, **в том числе контактная работа:** лекции 18 часов, практические занятия 18 часов, **самостоятельная работа:** 36 часов.

5. Перечень планируемых результатов обучения по дисциплине (или модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Планируемые результаты освоения образовательной программы (формируемые компетенции)	**Планируемые результаты обучения по дисциплине (модулю)**

Базовый уровень ПК-5. Способность участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	**Владеть:** навыками программирования алгебраических операций в конечных алгебраических структурах, в том числе в группе точек эллиптических и гиперэллиптических кривых, использования систем компьютерной математики для решения профессиональных задач; методами построения быстрых вычислительных алгоритмов алгебры и теории чисел. **Уметь:** проводить предварительное оценивание временной сложности разрабатываемых алгоритмов. **Знать:** принципы применения эллиптических и гиперэллиптических кривых в криптографии.
Базовый уровень ПК-10. Способность оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации.	**Владеть:** необходимыми теоретическими знаниями в областях, связанных с оценкой эффективности реализации систем защиты информации и действующих политик безопасности в компьютерных системах. **Уметь:** оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах. **Знать:** современные программно-аппаратные средства защиты информации, включая средства криптографической защиты информации.
Базовый уровень ПК-18. Способность способностью производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем,	**Владеть:** практическими навыками установки, наладки, тестирования и обслуживания современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем. **Уметь:** производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем. **Знать:** современные программно-аппаратные

включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации.	средства обеспечения информационной безопасности компьютерных систем, включая средства криптографической защиты информации.

6. Форма промежуточной аттестации:
зачёт.

7. Язык преподавания русский**.**

II. Содержание дисциплины (или модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

1. Для студентов очной формы обучения

Учебная программа – наименование разделов и тем	**Всего (час.)**	**Контактная работа (час.)**		**Самостоятельная работа (час.)**
		Лекции	Практические (лабораторные) занятия	
Раздел 1. Элементы алгебраической геометрии и алгебры				
Тема 1.1. Алгебраические структуры в криптографии	4	1	1	2
Тема 1.2. Понятие эллиптической кривой	4	1	1	2
Тема 1.3. Эллиптические кривые над числовыми полями	4	1	1	2
Тема 1.4. Эллиптические кривые над конечными полями	4	1	1	2
Тема 1.5. Группа точек эллиптической кривой	4	1	1	2
Раздел 2. Эллиптические кривые в криптографии	0			
Тема 2.1. Уравнения эллиптической кривой в краткой форме	4	1	1	2
Тема 2.2. Требования к эллиптическим кривым в криптографии	4	1	1	2
Тема 2.3. Шифрование с использованием эллиптических кривых	4	1	1	2
Тема 2.4. Обмен ключами с	4	1	1	2

использованием эллиптических кривых				
Тема 2.5. ЭЦП с использованием эллиптических кривых	4	2	2	2
Тема 2.6. Другие приложения эллиптических кривых в криптографии	4	1	1	2
Раздел 3. Вычислительные операции и задача дискретного логарифмирования на эллиптической кривой	0			
Тема 3.1. Классификация конечных полей и оценки сложности вычислительных операций	4	1	1	2
Тема 3.2. Особенности реализации на ЭВМ криптосистем на эллиптических кривых.	4	1	1	2
Тема 3.3.Алгоритмы дискретного логарифмирования на эллиптической кривой.	16	4	4	8
ИТОГО	**72**	**18**	**18**	**36**

Учебная программа

Раздел 1. ЭЛЕМЕНТЫ АЛГЕБРАИЧЕСКОЙ ГЕОМЕТРИИ И АЛГЕБРЫ

Тема 1.1. Алгебраические структуры в криптографии

Группы, кольца, поля. Порядок элемента и группы, характеристика поля. Образующий элемент. Расширение поля. Поля характеристики 2.

Тема 1.2. Понятие эллиптической кривой

Понятие эллиптической кривой. Порядок кривой. Нормальные формы эллиптической кривой. Особые и не особые точки эллиптической кривой. Параметризация эллиптической кривой, проективная плоскость и проективное пространство. Дискриминант и j-инвариант кривой. Изоморфизмы и эндоморфизмы эллиптических кривых. Гиперэллиптические и суперсингулярные кривые.

Тема 1.3. . Эллиптические кривые над числовыми полями

Эллиптические кривые над полем вещественных чисел, комплексных чисел, рациональных чисел. Геометрическое представление кривой над полем R.

Тема 1.4. Эллиптические кривые над конечными полями

Эллиптические кривые над полями F_p и F_q. Эллиптические кривые над полями характеристики 2 и 3. Число точек эллиптической кривой над конечным полем.

Тема 1.5. Группа точек эллиптической кривой

Закон сложения. Группа точек эллиптической кривой. Умножение точки на число. Задача дискретного логарифмирования на эллиптической кривой.

Раздел 2. ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ В КРИПТОГРАФИИ

Тема 2.1. Уравнения эллиптической кривой в краткой форме

Уравнение в краткой форме для полей характеристики отличной от 2 и 3. Уравнения в краткой форме для поля характеристики 2, 3.

Тема 2.2. Требования к эллиптическим кривым в криптографии

Основные требования к эллиптическим кривым и её параметрам в криптографии. Выбор эллиптической кривой и точки. Рекомендации NIST. Эллиптические кривые не пригодные для использования в криптографии.

Тема 2.3. Шифрование с использованием эллиптических кривых

Шифрование на базе эллиптических кривых. Встраивание открытого текста в точку кривой. Аналог RSA на эллиптических кривых. Аналог системы Мэсси-Омуры.

Тема 2.4. Обмен ключами с использованием эллиптических кривых

Аналог протокола Диффи-Хелмана с использованием эллиптических кривых.

Тема 2.5. ЭЦП с использованием эллиптических кривых

ЭЦП с использованием эллиптических кривых зарубежные стандарты. ЭЦП ГОСТ 34.10-2001. ЭЦП ГОСТ Р 34.10-2012. Сравнение отечественные стандарты ЭЦП с использованием эллиптических кривых.

Тема 2.6. Другие приложения эллиптических кривых в криптографии

Проверка чисел на простоту с использованием эллиптических кривых. P-1 метод Полларда, Алгоритм Ленстры.

Раздел 3. ВЫЧИСЛИТЕЛЬНЫЕ ОПЕРАЦИИ И ЗАДАЧА ДИСКРЕТНОГО ЛОГАРИФМИРОВАНИЯ НА ЭЛЛИПТИЧЕСКОЙ КРИВОЙ

Тема 3.1. Классификация конечных полей и оценки сложности вычислительных операций

Классификация конечных полей, используемых в криптографических приложениях. Теоретические оценки сложности вычислительных операции в конечных полях.

Тема 3.2. Особенности реализации на ЭВМ криптосистем на эллиптических кривых.

Особенности реализации криптосистем на эллиптических кривых на 32 бит ЭВМ. Быстрая арифметика для эллиптических кривых.

Тема 3.3. Алгоритмы дискретного логарифмирования на эллиптической кривой.

Универсальные методы дискретного логарифмирования. Метод Гельфонда. Методы встречи посередине и «giant step — baby step». Метод Полларда. Другие методы дискретного логарифмирования на эллиптической кривой.

III. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (или модулю)

Самостоятельная работа обучающихся направлена на освоение учебного материала и развитие практических умений. Самостоятельная работа включает следующие виды самостоятельной работы студентов: работа с рекомендованной литературой и документацией; выполнение практических заданий; подготовка к контрольным .

Список практических заданий

1. Доказать, что {0} обоазует коммукативную группу по «+»
2. Доказать, что $\{-1, +1\}$ образуют коммукативную группу по «+»
3. Проверить, принадлежит ли точка $(1; 7)$ прямой $E(F_{23}),\ y^2 = x^3 + x + 1\ \ (mod\ 23)$.

4. Проверить, что точка $P = (2; 7)$ принадлежат кривой $E(F_{11}), y^2 = x^3 + x + 6 \pmod{11}$

5. Проверить, что точка (1,3) принадлежат кривой $y^2 = x^3 + 2x + 6$, заданной над полем $\boldsymbol{F_7}$

Вопросы для контрольных тестов и самоконтроля.

1. Что такое группа, поле?
здесь должен быть ответ

2. Порождающий элемент группы, порядок группы, порядок элемента?
здесь должен быть ответ

3. Уравнение эллиптической кривой в краткой форме для поля характеристики не равной 2 и 3.
здесь должен быть ответ

4. Уравнение эллиптической кривой для полей характеристики 2 и 3.
здесь должен быть ответ

5. Группа точек эллиптической кривой.

6. Геометрическая интерпретация сложения точек эллиптической кривой

7. Порядок эллиптической кривой

8. Задача дискретного логарифмирования на эллиптической кривой

9. Назовите алгоритмы и (или) методы решения задача дискретного логарифмирования на эллиптической кривой

10. Назовите отечественный стандарт ЭЦП на эллиптической кривой

11. Умножение точки эллиптической кривой на число.

IV. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (или модулю)

1. Типовые контрольные задания для проверки уровня сформированности компетенций

Рассматривается трехкомпонентной структура компетенции: знать, уметь, владеть.

При этом под указанными категориями понимается:

- «знать» – воспроизводить и объяснять учебный материал с требуемой степенью научной точности и полноты;
- «уметь» – решать типичные задачи на основе воспроизведения стандартных алгоритмов решения;
- «владеть» – решать усложненные задачи на основе приобретенных знаний, умений и навыков, в нетипичных ситуациях

Этап формирования компетенции, в котором участвует дисциплина	**Типовые контрольные задания для оценки знаний, умений, навыков (2-3 примера)**	**Показатели и критерии оценивания компетенции, шкала оценивания**
Базовый		
владеть	вычислениями в заданной алгебраической структуре	• Имеется полное верное решение, включающее правильный ответ – 3 балла • Дано верное решение, но в решении имеются неверные записи, не отделенные от решения – 2 балла • Имеется верное решение части описания из-за логической ошибки – 1 балл • Решение не дано ИЛИ дано неверное решение – 0 баллов
	Алгоритмами реализующими вычислительные операции	• Имеется полное верное решение, включающее правильный ответ – 3 балла • Дано верное решение, но в решении имеются неверные записи, не отделенные от решения – 2 балла • Имеется верное решение части программы из-за логической ошибки – 1 балл • Решение не дано ИЛИ дано неверное решение – 0 баллов

уметь	Составлять и описывать алгоритмы реализующие вычисления заданной алгебраической структуре	• Факты и примеры в полном объеме обосновывают выводы – 2 балла • Допущена фактическая ошибка, не приведшая к существенному искажению смысла – 1 балл • Допущены фактические и логические ошибки, свидетельствующие о непонимании темы – 0 баллов
	Определить Порядок элемента, эллиптической кривой.	• Имеется полное верное решение, включающее правильный ответ – 3 балла • Дано верное решение, но в решении имеются неверные записи, не отделенные от решения – 2 балла • Имеется верное решение части программы из-за логической ошибки – 1 балл • Решение не дано ИЛИ дано неверное решение – 0 баллов
знать	Способы задания (описания) конечных полей, эллиптических кривых, группы.	• Факты и примеры в полном объеме обосновывают выводы – 2 балла • Допущена фактическая ошибка, не приведшая к существенному искажению смысла – 1 балл • Допущены фактические и логические ошибки, свидетельствующие о непонимании темы – 0 баллов
	Параметры эллиптических кривых влияющих на криптостойкость	• Факты и примеры в полном объеме обосновывают выводы – 2 балла • Допущена фактическая ошибка, не приведшая к существенному искажению смысла – 1 балл • Допущены фактические и логические ошибки, свидетельствующие о непонимании темы – 0 баллов
владеть	навыками доказательств	• Факты и примеры в полном объеме обосновывают выводы – 2

	утверждений и теорем	балла • Допущена фактическая ошибка, не приведшая к существенному искажению смысла – 1 балл • Допущены фактические и логические ошибки, свидетельствующие о непонимании темы – 0 баллов
уметь	Формулировать (описывать) алгоритмы реализующие криптографические системы на эллиптических кривых	• Имеется полное верное решение, включающее правильный ответ – 3 балла • Дано верное решение, но в решении имеются неверные записи, не отделенные от решения – 2 балла • Имеется верное решение части программы из-за алгоритмической ошибки – 1 балл • Решение не дано ИЛИ дано неверное решение – 0 баллов
знать	Стандарты криптосистем на эллиптических кривых	• Факты и примеры в полном объеме обосновывают выводы – 2 балла • Допущена фактическая ошибка, не приведшая к существенному искажению смысла – 1 балл • Допущены фактические и логические ошибки, свидетельствующие о непонимании темы – 0 баллов
	Требования (рекомендации) к эллиптическим кривым	• Факты и примеры в полном объеме обосновывают выводы – 2 балла • Допущена фактическая ошибка, не приведшая к существенному искажению смысла – 1 балл Допущены фактические и логические ошибки, свидетельствующие о непонимании темы – 0 баллов

При оценивании результатов освоения дисциплины применяется «рейтинговая» технология (балльно-накопительная) система. Оценка уровня

сформированности компетенций осуществляется в процессе следующих форм контроля:

1) **следящего** (проводится оценка выполнения студентами заданий в ходе аудиторных занятий). Дает возможность квалифицировать степень сформированности знаний, умений, навыков, а также их глубину и прочность. Его задача - регулярное управление учебной деятельности студентов и ее корректировка. Он позволяет получать первичную информацию о ходе и качестве усвоения учебного материала, а также стимулировать регулярную, напряженную и целенаправленную работу студентов. Данный контроль позволяет вовремя выявить пробелы в знаниях и оказать им помощь в усвоении программного материала. Данными формами контроля являются: ответы с места и у доски, проверка работ выполненных в тетради.

2) **текущего** (оценивается работа студентов вне аудиторных занятий). Текущими формами контроля являются: проверка выполнения практических работ, ответы у доски, рефераты, доклады, проверка самостоятельной работы студентов.

3) **промежуточного** (рейтинговые точки) позволяет определять качество изучения студентами учебного материала по разделам и темам. Контроль проводится два раз в семестр. С помощью периодического контроля обобщаются и усваиваются целые темы и разделы, выявляется взаимосвязями с другими разделами, предметами. Контроль охватывает студентов и всей группы и проводится в виде теста, письменных практических работ.

4) **итогового** (зачёт). Максимальная сумма рейтинговых баллов по дисциплине составляет 100 баллов. Студенту, набравшему 50 баллов и выше по итогам работе в семестре, в экзаменационной ведомости и зачетной книжке выставляется оценка «зачтено». Студент, набравший от 20 до 49 баллов включительно, сдаёт зачет в последнюю неделю семестра по данной дисциплине. Баллы, полученные на зачете проставляются в ведомости. Студенту, набравшему меньше 20 баллов, в экзаменационной ведомости выставляется оценка «незачтено». Данному студенту разрешается пересдача зачета по направлению деканата на последней неделе семестра.

Формы контроля

Занятия для студентов очной формы обучения проводятся в 1-м семестре 5 курса и заканчиваются зачетом. Период времени, отведенный на обучение по данной дисциплине, планируется разделить на 2 модуля, каждый из которых заканчивается контрольной точкой. Количество баллов за текущую работу выставляется в соответствии со сложностью темы и количеством заданий, выносимых для практических работ в аудитории и самостоятельных занятий.

Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций в процессе освоения образовательной программы.

Для оценки уровня теоретических и практических знаний используется тест или контрольная работа письменный опрос. Перечень некоторых вопросов теста и практических заданий представлен ниже.

Приводится два варианта из имеющихся двадцати различных вариантов по каждой из рассматриваемых тем.

Вариант 1

1.Проверить, что точки (1,3); (2,4); (5,2) принадлежат кривой $y^2 = x^3 + 2x + 6$, заданной над полем $\boldsymbol{F_7}$

2. **Для кривой $y^2 = x^3 + x + 6$ над $\boldsymbol{F_{11}}$ найти P+Q, если P(1,8); Q(1,8)**

Вариант 2

1.Проверить, что точки (4,6); (3,2); (2,2) принадлежат кривой $y^2 = x^3 + 2x + 6$, заданной над полем $\boldsymbol{F_7}$

2. **Для кривой $y^2 = x^3 + x + 6$ над $\boldsymbol{F_{11}}$ найти P+Q, если P(8,3); Q(3,6)**

ВОПРОСЫ К ЗАЧЕТУ 9 СЕМЕСТР

1. Понятие эллиптической кривой над числовым полем. Группа точек эллиптической кривой
2. Понятие эллиптической кривой над конечным полем. Группа точек эллиптической кривой
3. Эллиптические кривые в криптографии
4. Вычислительные операции в конечных полях
5. Системы шифрования на эллиптических кривых
6. Обмен ключами с использованием эллиптических кривых
7. Протокол Диффи – Хелмана на основе суперсингулярных кривых
8. ЭЦП на эллиптических кривых
9. Алгоритмы генерации эллиптической кривой и выбора точки на ней
10. Задача дискретного логарифмирования на эллиптической кривой
11. Число точек эллиптической
12. Встраивание открытого текста в координату точки
13. Требования к эллиптической кривой
14. Метод Гельфонда
15. Методы встречи посередине
16. Метод Полларда
17. Алгоритм Шенкса

V. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (или модуля)

а) Основная литература

Рацеев, С. М. Математические методы защиты информации / С. М. Рацеев. — 2-е изд., стер. — Санкт-Петербург : Лань, 2023. — 544 с. — ISBN 978-5-507-47085-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/326153

Алешников С.И. Математические методы защиты информации. Часть 5. Методы алгебраических кривых [Электронный ресурс]: учебное пособие/ С.И. Алешников,

А.А.Смирнов. - М. ; Берлин : Директ-Медиа, 2017. - 358 с. : ил., табл. - Библиогр. в кн. - ISBN 978-5-4475-8780-2 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=457616

б) Дополнительная литература:

Фороузан, Б. А. Криптография и безопасность сетей : учебное пособие для СПО / Б. А. Фороузан ; под редакцией А. Н. Берлина. — Саратов : Профобразование, 2021. — 776 с. — ISBN 978-5-4488-0999-6. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/102192.html

Донгак, Ш. М. Криптография: Практикум : учебное пособие / Ш. М. Донгак. — Москва : РТУ МИРЭА, 2020 — Часть 2 — 2020. — 64 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/163935

VI. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (или модуля)

1. ЭБС Лань https://e.lanbook.com/ Договор № 4-е/23 от 02.08.2023 г.
2. ЭБС Znanium.com https://znanium.com/ Договор № 1106 эбс от 02.08.2023 г.
3. ЭБС Университетская библиотека online https://biblioclub.ru Договор № 02-06/2023 от 02.08.2023 г.
4. ЭБС ЮРАЙТ https://urait.ru/ Договор № 5-е/23 от 02.08.2023 г.
5. ЭБС IPR SMART https://www.iprbookshop.ru/ Договор № 3-е/23К от 02.08.2023 г.
6. https://cyberleninka.ru/ научная электронная библиотека «Киберленинка».
7. Научная электронная библиотека eLIBRARY.RU (подписка на журналы) https://elibrary.ru/projects/subscription/rus_titles_open.asp;
8. Репозитарий ТвГУ http://eprints.tversu.ru

VII. Методические указания для обучающихся по освоению дисциплины (или модуля)

Материал дисциплины распределен по главным разделам (темам). В результате изучения дисциплины у студентов должно сформироваться научное представление о криптографических системах на базе эллиптических кривых. Необходимо выработать системный подход к пониманию процессов преобразования входных данных в приложениях защиты информации. В процессе обучения студенты, наряду с текстами лекций и учебными пособиями, должны пользоваться дополнительными научными изданиями, академическими периодическими изданиями. После каждой лекционной темы рекомендуется проработать вопросы для повторения и самоконтроля. В аспекте самостоятельной работы рекомендуется составлять конспект. Рекомендуется использовать справочники и руководства.

Для успешного освоения дисциплины важно соблюсти следующие рекомендации: На первой лекции важно обратить внимание на конкретные требования к прохождению и сдаче курса. Активная работа на занятиях, выполнение творческих заданий сформирует о Вас дополнительное положительное представление как об активном участнике познавательного процесса. На данном курсе практические занятия являются самым важным компонентом обучающего процесса. На занятиях будет представлен необходимый теоретически материал по темам и представлены практические задания для решения на занятиях в аудитории под руководством преподавателя и самостоятельно. Многие задачи являются стандартными и имеют уже готовые шаблоны (алгоритмы) решения, тем не менее, для получения большего познавательного и учебного эффекта, настоятельно рекомендуется написание собственного оригинального кода.

Самостоятельная работа студентов в рамках данной дисциплины в основном состоит в подготовке к практическим занятиям и работе с разными источниками. Освоению учебного материала большую помощь окажет личный творческий подход, связанный с дополнительным просмотром материала по отдельным темам в библиотеках и системе «Интернет». Самостоятельная работа является необходимой на всей стадиях и при всех формах изучения предмета. Важно помнить: без самостоятельной работы невозможно серьезное освоение любого курса. Надо быть готовым к тому, что по времени, затраченном на дисциплину, самостоятельная работа будет превалировать над иными видами работы. Важно продумать стиль фиксации нового и важного материала. Рекомендуется немедленно обсуждать любые возникшие в процессе обучения вопросы, проблемы и неясности с преподавателем, не откладывая это обсуждение до контрольной точки. Проконсультироваться с преподавателем можно во время и после практических занятий, во время консультаций, а также по электронной почте.

VIII. Перечень педагогических и информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (или модулю), включая перечень программного обеспечения и информационных справочных систем (по необходимости)

Процесс изучения дисциплины включает лекции, практические занятия и самостоятельную работу студента. Во время обучения применяется контактная технология преподавания (за исключением самостоятельно изучаемых студентами вопросов). При проведении занятий применяется имитационный подход (метод деловой игры, анализ конкретных ситуаций), когда преподавателем разбирается на конкретном примере проблемная ситуация, все шаги решения задачи студентам демонстрируются при помощи мультимедийной техники. Затем студенты самостоятельно решают аналогичные задания. Так же при проведении занятий применяется частично-поисковый метод: студенты осуществляют поиск решения поставленной проблемы (задачи). При этом постановочные задачи опираются на уже имеющиеся у студентов знания и умения, полученные в предшествующих темах. На занятиях практикуется выполнение заданий в малых группах, письменные работы, работа с раздаточным материалом, привлекаются ресурсы сети Интернет. Курс предусматривает выполнение тестов, контрольных и самостоятельных работ, письменных домашних заданий. В качестве форм контроля используются различные варианты взаимопроверки и взаимоконтроля.

Программное обеспечение

Google Chrome	бесплатно
Kaspersky Endpoint Security 10 для Windows	Акт на передачу прав ПК545 от 16.12.2022
Lazarus	бесплатно
OpenOffice	бесплатно
Многофункциональный редактор ONLYOFFICE бесплатное ПО	бесплатно
ОС Linux Ubuntu бесплатное ПО	бесплатно

IX. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине (или модулю)

Учебная аудитория с мультимедийной установкой (Ноутбук, проектор, колонки), наличие классной доски.. Класс ПЭВМ.

X. Сведения об обновлении рабочей программы дисциплины (или модуля)

№п.п.	Обновленный раздел рабочей программы дисциплины (или модуля)	Описание внесенных изменений	Дата и протокол заседания кафедры, утвердившего изменения
1.	I - X	14.05.2017 Корректировка всех разделов в соответствии с новым стандартом	
2.			
3.			