БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

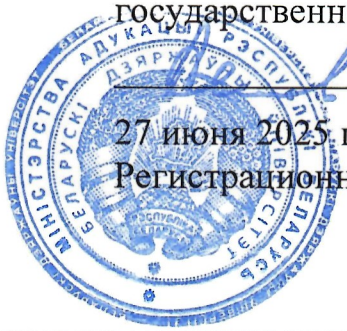
УТВЕРЖДАЮ

Ректор Белорусского
государственного университета

_____А.Д.Король

27 июня 2025 г.

Регистрационный № 3564/б.



МАТЕМАТИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ

Учебная программа учреждения образования по учебной дисциплине для специальности:

6-05-0533-08 Компьютерная математика и системный анализ

2025 г.

Учебная программа составлена ОСВО 6-05-0533-08-2023, учебных планов БГУ № 6-5.4-56/01 от 15.05.2023, № 6-5.4-56/11ин. от 31.05.2023.

СОСТАВИТЕЛИ:

А.В.Кушнеров, старший преподаватель кафедры дифференциальных уравнений и системного анализа механико-математического факультета Белорусского государственного университета

РЕЦЕНЗЕНТЫ:

А.А.Перхунов, начальник отдела разработки программного обеспечения управления цифровизации РУП «Производственное объединение Белоруснефть»

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой дифференциальных уравнений и системного анализа БГУ (протокол № 14 от 05.06.2025)

Научно-методическим советом БГУ (протокол № 11 от 26.06.2025)

Заведующий кафедрой _____ Л.Л.Голубева

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Цели и задачи учебной дисциплины

Цель учебной дисциплины – обучение студентов основным математическим понятиям и алгоритмам, которые используются в криптографии.

Образовательная цель: обучение студентов приёмам построения современных криптосистем.

Развивающая цель: освоение практических навыков в прикладной линейной алгебре и построении алгоритмов.

Задачи учебной дисциплины:

– формировать у студентов глубокое понимание математических объектов, используемых в криптографии;

– развивать способности реализации алгоритмов на языках программирования Wolfram Language и Python;

– обучить студентов основным объектам криптографии: криптосистемам, функциям хеширования, электронным цифровым подписям.

Место учебной дисциплины в системе подготовки специалиста с высшим образованием.

Учебная дисциплина «Математические основы защиты информации» относится к модулю «Компьютерное моделирование» компонента учреждения образования.

Связи с другими учебными дисциплинами, включая учебные дисциплины компонента учреждения высшего образования, дисциплины специализации и др.

Учебная программа составлена с учетом программ по дисциплинам: «Алгебра и теория чисел», «Теория помехоустойчивого кодирования».

Требования к компетенциям

Освоение учебной дисциплины «Математические основы защиты информации» должно обеспечить формирование следующей компетенции**:**

Специализированные компетенции:

Осуществлять математическое и прикладное моделирование для математических исследований.

В результате освоения учебной дисциплины студент должен:

знать:

– основные симметричные и асимметричные криптосистемы;

– стандарты электронной цифровой подписи;

– типовые криптографические протоколы;

уметь:

– корректно применять основные криптосистемы;

– формировать электронную цифровую подпись под электронным документом;

иметь навык:

– шифрования и передачи информации;

– обеспечения целостности и аутентификации информации.

Структура учебной дисциплины

Дисциплина изучается в 5 и 6 семестрах. В соответствии с учебным планом всего на изучение учебной дисциплины «Математические основы защиты информации» отведено **для очной формы** получения высшего образования – 198 часов, в том числе 70 аудиторных часов, лекции – 34 часа, лабораторные занятия – 36 часов. **Из них:**

5 семестр:

Лекции – 18 часов, лабораторные занятия – 14 часов, управляемая самостоятельная работа (УСР) – 4 часа.

Трудоемкость учебной дисциплины составляет 3 зачетные единицы.

Форма промежуточной аттестации – зачёт.

6 семестр:

Лекции – 16 часов, лабораторные занятия – 14 часов, управляемая самостоятельная работа (УСР) – 4 часа.

Трудоемкость учебной дисциплины составляет 3 зачетные единицы.

Форма промежуточной аттестации – экзамен.

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Тема 1. Основные алгоритмы теории чисел.

Алгоритм Евклида, расширенный алгоритм Евклида, возведение в степень в кольце классов вычетов. Вычисление обратных элементов в мультипликативной группе кольца классов вычетов.

Тема 2. Генерация простых чисел.

Решето Эратосфена. Малая теорема Ферма. Псевдопростые числа. Числа Кармайкла. Свидетели простоты. Вероятностный тест на простоту Миллера-Рабина. Теорема Диемитко. Детерминированный полиномиальный алгоритм проверки простоты чисел. Детерминированный и вероятностный алгоритмы. Алгоритм Монте-Карло.

Тема 3. Алгебраические уравнения в кольце вычетов.

Уравнение первой степени. Китайская теорема об остатках. Алгоритм Гаусса. Алгоритм Гарнера. Квадратичный вычет. Квадратичный невычет. Символ Лежандра. Символ Якоби. Вычисление символа Якоби при помощи квадратичного закона взаимности Гаусса. Алгоритм Шенкса. Квадратное уравнения в случае составного модуля. Числа Блюма. Алгоритм Лас-Вегаса.

Тема 4. Факторизация чисел.

Метод пробных делений. Парадокс дней рождения. Ро-метод Полларда. (p-1)-алгоритм Полларда. Классы P и NP. Факторизация Ферма и факторные базы. Метод Диксона. Факторизация методом квадратичного решета.

Тема 5. Криптосистемы с открытым ключом.

Парадокс симметричных криптосистем. Криптосистемы с открытым ключом. Односторонние функции. Односторонние функции с лазейкой. Криптосистема RSA. Эквивалентность задачи разложения модуля на множители и вычисления функции Эйлера. Эквивалентность задачи разложения модуля на множители и вычисления секретного показателя.

Тема 6. Дискретное логарифмирование. Криптосистема Эль-Гамаля.

Определение дискретного логарифма. Образующий элемент. Алгоритм больших и малых шагов. Алгоритм Полига-Хеллмана.

Тема 7. Конечные поля.

Поле. Конечное поле. Способы задания конечных полей. Вычисления в конечных полях. Неприводимые полиномы над полем. Мультипликативная группа поля. Цикличность мультипликативной группы поля.

Тема 8. Криптостандарт AES.

Алгоритм шифрования AES. Математические основы работы алгоритма шифрования. Блочное шифрование. Протокол обмена ключами. Симметричные и ассиметричные криптосистемы.

Тема 9. Функции хеширования.

Функции хеширования. Коллизии. Хранение паролей. Хранение и поиск данных. Хеш-таблицы. Алгоритм вычисления контрольной суммы. Контроль целостности данных. Криптографические функции хеширования.

Тема 10. Электронная цифровая подпись.

Электронная цифровая подпись. Электронная цифровая подпись Эль-Гамаля. Электронная цифровая подпись Шнорра.

Тема 11. Эллиптические кривые.

Определение эллиптической кривой. Дискриминант. Пересечение эллиптической кривой и прямой. Группа точек эллиптической кривой. Цикличность группы точек эллиптической кривой. Порядок группы точек эллиптической кривой. Алгоритм вычисления произведения натурального числа и точки эллиптической кривой. Дискретное логарифмирование на эллиптической кривой. Алгоритм больших и малых шагов. Алгоритм Полига-Хеллмана. Криптография с использованием эллиптических кривых.

Тема 12. Основы помехоустойчивого кодирования.

Понятие линейного кода. Порождающая и проверочная матрицы кода. Минимальное расстояние кода. Простейшие методы декодирвования.

Тема 13. Решетки.

Определение решетки. Базис решетки. Определитель решетки. Ортогонализация Грама-Шмидта. LLL-приведенный базис и его свойства. LLL-алгоритм. Атаки на криптосистему RSA при помощи решеток. Атака Хастада. Результант многочленов. Атака Франклина-Райтера.

Тема 14. Криптографические протоколы.

Схемы обязательств. Обмен ключами Диффи-Хеллмана. Доказательства с нулевым разглашением. Разделение секрета.

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ

Очная форма получения высшего образования с применением дистанционных образовательных технологий (ДОТ)

Номер раздела, темы	Название раздела, темы	Количество аудиторных часов					Количество часов УСР	Форма контроля знаний
		Лекции	Практические занятия	Семинарские занятия	Лабораторные занятия	Иное		
1	2	3	4	5	6	7	8	9
	5 семестр	**18**			**14**		**4**	
1	Основные алгоритмы теории чисел.	2			2			Отчет по лабораторной работе с устной защитой.
2	Генерация простых чисел	2			2			Отчет по лабораторной работе с устной защитой.
3	Алгебраические уравнения в кольце вычетов.	2			2		2	Отчет по лабораторной работе с устной защитой, контрольная работа.
4	Факторизация чисел.	4			2			Отчет по лабораторной работе с устной защитой.
5	Криптосистемы с открытым ключом	4			2		2	Отчет по лабораторной работе с устной защитой, контрольная работа.
6	Дискретное логарифмирование. Криптосистема Эль-Гамаля.	4			4			Отчет по лабораторной работе с устной защитой, защитой.
	6 семестр	**16**			**14**		**4**	
7	Конечные поля.	2			2			Отчет по лабораторной работе с устной защитой.

8	Криптостандарт AES.	2			2			Отчет по лабораторной работе с устной защитой.
9	Функции хеширования.	2			2			Отчет по лабораторной работе с устной защитой.
10	Электронная цифровая подпись	2			2			Отчет по лабораторной работе с устной защитой.
11	Эллиптические кривые	2			2			Отчет по лабораторной работе с устной защитой.
12	Основы помехоустойчивого кодирования.	2			2		2	Отчет по лабораторной работе с устной защитой, контрольная работа.
13	Решетки.	2			2			Отчет по лабораторной работе с устной защитой
14	Криптографические протоколы	2					2	Устный опрос

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

Основная литература

1. Введение в теоретико-числовые методы криптографии : учеб. пособие / М. М. Глухов, И. А. Круглов, А. Б. Пичкур, А. В. Черемушкин. – Изд. 2-е, стер. – СПб. ; М. ; Краснодар : Лань, 2024. – 394 с. – URL: https://e.lanbook.com/book/397286 (дата обращения 03.10.2025).
2. Мартынов, Л. М. Алгебра и теория чисел для криптографии : учебное пособие [для вузов] / Л. М. Мартынов. – Изд. 2-е, стер. – СПб. ; М. ; Краснодар : Лань, 2022. – 454 с.
3. Криптология : учебник для студентов учреждений высшего образования по математическим и техническим специальностям / [Ю. С. Харин и др.] ; БГУ. – 2-е изд., пересмотр. – Минск : БГУ, 2023. – 511 с. – URL: https://elib.bsu.by/handle/123456789/309839 (дата обращения 03.10.2025).

Дополнительная литература

1. Фергюсон, Нильс Практическая криптография = Practical Cryptography / Нильс Фергюсон, Брюс Шнайер ; [пер. с англ. Н. Н. Селиной ; под ред. А. В. Журавлева]. - Москва; Санкт-Петербург; Киев: Диалектика, 2005. - 422с.
2. Математические и компьютерные основы криптологии: Учеб. пособие для студ. матем. и инженерно-техн. спец. вузов / Ю. С. Харин, В. И. Берник, Г. В. Матвеев, С. В. Агиевич. - Минск: Новое знание, 2003. - 381с.
3. Харин, Ю.С. Математические основы криптологии / Ю.С. Харин, В.И. Берник, Г.В. Матвеев. – Минск: БГУ, 1999. – 319 с.
4. Харин, Ю.С. Компьютерный практикум по математическим методам защиты информации: Учеб. пособие для студ. матем. и инженерно-технических спец. вузов / Ю.С.Харин, С.В.Агиевич. - Мн. : БГУ, 2001. - 190с.
5. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. 2-е издание / Брюс Шнайер. — М.: Триумф, 2002. — 816 с.
6. Menezes, A Handbook of Applied Cryptography / A. Menezes, P. van Oorschot and S. Vanstone. CRC Press, 1997. – 780 p.
7. Алферов, А.П. Основы криптографии. Учебное пособие, 2-е изд., испр. и доп. / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. – М.: Гелиос АРВ, 2002. – 480 с.
8. Болотов, А.А. Элементарное введение в эллиптическую криптографию: Алгебраические и алгоритмические основы / А.А. Болотов, С.Б. Гашков, А.Б. Фролов, А.А. Часовских. – М.: КомКнига, 2006. – 328 с.
9. Дориченко, С.А. 25 этюдов о шифрах / С.А. Дориченко, В.В. Ященко. – М.: ТЕИС, 1994. – 69 с.

10. Кнут, Д. Искусство программирования. Т. 2. Получисленные алгоритмы. 3-е издание. / Д. Кнут. – М.-СПб.-Киев: Вильямс, 2003.

11. Молдовян, А. А. Криптография / А. А. Молдовян, Н. А. Молдовян, Б. Я. Советов. – СПб. : Лань, 2001. – 224 с.

12. Нестеренко, Ю.В. Теория чисел: учебник для студ. высш. учеб. заведений / Ю.В. Нестеренко. – М.: Издательский центр «Академия», 2008. – 272 с.

13. Острик, В.В. Алгебраическая геометрия и теория чисел: рациональные и эллиптические кривые / В.В. Острик, М.А. Цфасман. – М.: МЦНМОб 2001. – 48 с.

14. Романец, Ю.В. Защита информации в компьютерных системах и сетях / Ю.В. Романец, П.А. Тимофеев, В.Ф. Шаньгин. – М.: Радио и связь, 2001. – 376 с.

15. Саломаа, А. Криптография с открытым ключом / – М.: Мир, 1996. – 320 с.

16. Птицын, Н. Приложение теории детерминированного хаоса в криптографии / Н. Птицын. – М.: МГТУ им. Н.Э. Баумана, 2002. – 80 с.

17. Василенко, О.Н. Теоретико-числовые алгоритмы в криптографии / О.Н. Василенко. – М.: МЦНМО, 2003. – 328 с.

18. Введение в криптографию / Под ред. В.В. Ященко. – М.: МЦНМО-ЧеРоб, 1998, 271 с.

19. Коблиц, Н. Курс теории чисел и криптографии / Н. Коблиц. – М.: Научное изд-во ТВП, 2001. – 254 с.

20. Мао, Венбо Современная криптография = Modern Cryptography : теория и практика / Венбо Мао ; [пер. с англ. и ред. Д. А. Клюшина]. - Москва; Санкт-Петербург; Киев: Вильямс, 2005. - 764с.

21. Смарт, Н. Криптография / Н. Смарт; пер. с англ. С. А. Кулешова под ред. С. К. Ландо. - Москва: Техносфера, 2006. - 525 с.

Перечень рекомендуемых средств диагностики и методика формирования итоговой отметки

Контроль работы студента проходит в форме опроса на лабораторных занятиях, а также во время устной защиты отчета по лабораторным работам. Также по ряду тем предусмотрены контрольные работы.

Отметка за ответы на лекциях и лабораторных занятиях включает в себя полноту ответа, наличие аргументов, примеров из практики, глубину понимания терминов, используемых студентом при ответе на вопросы.

При защите лабораторных работ ценится оригинальность кода, самостоятельность выполнения (самостоятельно выполненное задание, но с некоторыми шероховатостями, ценится выше, чем вышколенный отчет, похожий на отчет соседа). Также очень важно, чтобы реализованные студентом алгоритмы работали на больших числах, так как именно большие числа

используются в криптографии и именно на больших числах проявляется свойство полиномиальности алгоритма.

Формой промежуточной аттестации по дисциплине «Математические основы защиты информации» учебным планом предусмотрен зачет и экзамен.

Для формирования итоговой отметки по учебной дисциплине используется модульно-рейтинговая система оценки знаний студента, дающая возможность проследить и оценить динамику процесса достижения целей обучения. Рейтинговая система предусматривает использование весовых коэффициентов для текущей и промежуточной аттестации студентов по учебной дисциплине.

Формирование итоговой отметки в ходе проведения контрольных мероприятий текущей аттестации (примерные весовые коэффициенты, определяющие вклад текущей аттестации в отметку при прохождении промежуточной аттестации):

− отчёты по лабораторным работам с устной защитой – 60%;

− контрольные работы, устный опрос – 40%.

Итоговая отметка по дисциплине рассчитывается на основе итоговой отметки текущей аттестации (рейтинговой системы оценки знаний) 40% и экзаменационной отметки 60%.

Примерный перечень заданий для управляемой самостоятельной работы студентов

Тема 3. Алгебраические уравнения в кольце вычетов. (2 ч.)

Китайская теорема об остатках. Алгоритм Гаусса. Алгоритм Гарнера.

Реализовать в Mathematica или Python алгоритмы Гаусса и Гарнера. Сравнить практически скорость работы данных алгоритмов. Для каждого алгоритма найти количество арифметических операций, необходимых для выполнения всех шагов алгоритма. Являются ли данные алгоритмы полиномиальными?

Целью данного задания является выработка у студента навыков оценки сложности алгоритма.

Форма контроля – контрольная работа.

Тема 5. Криптосистемы с открытым ключом. (2 ч.)

Криптосистемы с открытым ключом. Односторонние функции. Односторонние функции с лазейкой. Криптосистема RSA. Эквивалентность задачи разложения модуля на множители и вычисления секретного показателя.

Исследовать работу функций GenerateAsymmetricKeyPair, Encrypt, Decrypt пакета Mathematica:

Какого размера может быть модуль n криптосистемы RSA?

Чему равна открытая экспонента по умолчанию. Для какой операции удобно пятое число Ферма? Можно ли задавать открытую экспоненту самому?

При помощи секретной экспоненты разложить модуль n на множители p, q. Найти количество бит чисел p и q. Всегда ли количество бит чисел p и q совпадает?

Форма контроля – контрольная работа.

Тема 12. Основы помехоустойчивого кодирования (2 ч.)

БЧХ -код (91,12 δ = 5) задан матрицей H2. При построении поля использован полином $1+\alpha+\alpha^2+\alpha^{10}+\alpha^{12}$.

Примерный перечень заданий:

Исправить ошибки, принятые декодером с пр. матрицей H2 методом систем и уравнения (1 и 2 сообщения).

Вывести позиции ошибочных меток. Вывести все промежуточные вычисления.

Позиции ошибок в 3-ем сообщении отыскать любым способом.

Форма контроля – контрольная работа.

Тема 14. Криптографические протоколы (2ч.)

Определение дискретного логарифма. Образующий элемент. Алгоритм Полига-Хеллмана.

Реализовать алгоритм Полига-Хеллмана. Посчитать количество арифметических операций для данного алгоритма. Является ли он полиномиальным? От каких свойств модуля зависит скорость работы алгоритма? При разработке криптосистем, стойкость которых основана на проблеме вычисления дискретного логарифма, каким свойством должен обладать модуль?

Форма контроля – устный опрос.

Описание инновационных подходов и методов к преподаванию учебной дисциплины

При организации образовательного процесса используется ***практико-ориентированный подход,*** который предполагает освоение содержания через решения практических задач.

При организации образовательного процесса ***используются методы и приемы развития критического мышления,*** которые представляют собой систему, формирующую навыки работы с информацией в процессе чтения и письма; понимании информации как отправного, а не конечного пункта критического мышления.

Методические рекомендации по организации самостоятельной работы обучающихся

Для организации самостоятельной работы студентов по учебной дисциплине рекомендовано разместить на образовательном портале (https://edummf.bsu.by/course/view.php?id=1095) или сайте кафедры

(https://km.mmf.bsu.by/education.html) учебно-методические материалы: методические указания к лабораторным занятиям, вопросы для подготовки к экзамену, перечень рекомендуемой литературы, информационных ресурсов.

Примерный перечень вопросов зачету

1. Полиномиальный, экспоненциальный и субэкспоненциальный алгоритмы.
2. Нахождение обратного относительно умножения элемента в кольце вычетов.
3. Быстрое возведение в степень в кольце вычетов.
4. Теорема Эйлера.
5. Малая теорема Ферма.
6. Числа Кармайкла.
7. Свидетели простоты числа.
8. Тест на простоту Миллера-Рабина.
9. Теорема Диемитко.
10. Детерминированный и вероятностный алгоритмы
11. Постановка задачи факторизации.
12. Метод факторизации Ферма.
13. Метод пробных делений.
14. ρ-метод Полларда.
15. ρ-метод Полларда с генерацией последовательности.
16. ρ-метод Полларда с генерацией последовательности. Черепаха и Заяц.
17. ρ-метод Полларда с генерацией последовательности. Черепаха и Ахиллес.
18. Классы сложности *P; NP:*
19. Китайская теорема об остатках.
20. Алгоритм Гарнера.
21. Квадратичный вычет.
22. Символ Лежандра и Якоби.
23. Алгоритм Шенкса.
24. Односторонние функции и односторонние функции с лазейкой.
25. Криптосистемы с открытым ключом.
26. Криптосистема *RSA.*
27. Корректность *RSA*
28. Применение китайской теоремы об остатках при вычислениях в RSA.
29. Цепные дроби.
30. Дискретный логарифм
31. Вычисление образующего элемента в мультипликативной группе кольца вычетов.
32. Алгоритм больших и малых шагов.

33. Алгоритм Полига-Хеллмана.
34. Криптосистема Эль-Гамаля.
35. Криптостойкость симметричных криптосистем.

Примерный перечень вопросов к экзамену

1. Полиномиальный, экспоненциальный и субэкспоненциальный алгоритмы.
2. Нахождение обратного относительно умножения элемента в кольце вычетов.
3. Быстрое возведение в степень в кольце вычетов.
4. Теорема Эйлера и Малая теорема Ферма.
5. Числа Кармайкла.
6. Тест на простоту Миллера-Рабина.
7. Теорема Диемитко.
8. Детерминированный и вероятностный алгоритмы
9. Функция хеширования. Ее применение.
10. Криптографическая функция хеширования.
11. Алгоритм вычисления контрольной суммы.
12. Функция хеширования MD-5.
13. ρ-метод Полларда.
14. Классы сложности *P; NP:*
15. Китайская теорема об остатках. Алгоритм Гарнера.
16. Квадратичный вычет. Символ Лежандра и Якоби.
17. Алгоритм Шенкса.
18. Односторонние функции и односторонние функции с лазейкой.
19. Криптосистемы с открытым ключом.
20. Криптосистема *RSA*
21. Цепные дроби.
22. Дискретный логарифм
23. Вычисление образующего элемента в мультипликативной группе кольца вычетов.
24. Алгоритм больших и малых шагов.
25. Алгоритм Полига-Хеллмана.
26. Криптосистема Эль-Гамаля.
27. Электронная цифровая подпись.
28. Цифровая подпись Эль-Гамаля.
29. Цифровая подпись Шнорра.
30. Эллиптические кривые.
31. Аддитивная абелева группа точек эллиптической кривой.
32. Конечные поля.
33. Вычисления в конечных полях.
34. Криптосистема AES.
35. Основы помехоустойчивого кодирования.

36. Проверочная и порождающая матрица кода. Минимальное расстояние кода.
37. Код Хемминга.
38. Синдромный метод исправления ошибок.
39. Декодирование в ближайшее кодовое слово.
40. Криптографические протоколы

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ УО

Название учебной дисциплины, с которой требуется согласование	Название кафедры	Предложения об изменениях в содержании учебной программы учреждения высшего образования по учебной дисциплине	Решение, принятое кафедрой, разработавшей учебную программу (с указанием даты и номера протокола)
Теория помехоустойчивого кодирования	Кафедра дифференциальных уравнений и системного анализа	Предложения отсутствуют	Рекомендовать к утверждению учебную программу (протокол № 14 от 05.06.2025)

Заведующий кафедрой дифференциальных
уравнений и системного анализа
к.ф.-м.н., доцент _____ Л.Л.Голубева

05.06.2025

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ К УЧЕБНОЙ ПРОГРАММЕ УО

на _____/_____ учебный год

№ п/п	Дополнения и изменения	Основание

Учебная программа пересмотрена и одобрена на заседании кафедры
_____ (протокол № ____ от _____ 202_ г.)

Заведующий кафедрой
_____ _____

УТВЕРЖДАЮ
Декан факультета
_____ _____