Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Матвеев Александр Валерьевич
Должность: Проректор по образовательной деятельности
Дата подписания: 04.08.2026 15:06:18
Уникальный программный ключ:
287d28879a9eafccca070f6fe8b2fd87c7444eca

МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Вологодский государственный университет»

УТВЕРЖДАЮ
Проректор по образовательной деятельности
_____Матвеев А.В.
« » 2026 г.

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Направление подготовки / специальность: 09.03.01 Информатика и вычислительная техника

Направленность (профиль / специализация): Программное обеспечение средств вычислительной техники и информационной безопасности

Квалификация выпускника: бакалавр

Форма обучения: Очная

Институт: математики, естественных и компьютерных наук

Кафедра: автоматики и вычислительной техники

Вологда
2026 г.

Составитель рабочей программы
доцент, ктн, доцент _ / Тихомирова Е.Н. /

Рабочая программа дисциплины **Криптографические методы защиты информации** разработана в соответствии с ФГОС ВО по направлению подготовки/специальности 09.03.01 Информатика и вычислительная техника, направленность (профиль) Программное обеспечение средств вычислительной техники и информационной безопасности.

Составлена на основании учебного плана направления подготовки 09.03.01 Информатика и вычислительная техника, направленность Программное обеспечение средств вычислительной техники и информационной безопасности.

Рабочая программа рассмотрена на заседании кафедры Автоматики и вычислительной техники

Заведующий кафедрой _ /Суконщиков А.А. /

Рабочая программа одобрена на заседании методического совета института ИМЕКН

Протокол от «14» мая 2026 г. № 8.

Председатель методического совета /Голубев О.Б./

СОГЛАСОВАНО:

Председатель рабочей группы
по УГНС 09.00.00 _ / Суконщиков А.А./

1. ЦЕЛИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целями освоения учебной дисциплины являются

1. изучение студентами указанных методов и развитие навыков решения задач криптографии
2. освоение фундаментальных математических понятий криптологии;
3. освоение базовых математических алгоритмов и методов, лежащих в основе методов защиты информации;
4. изучение подходов к созданию современных криптосистем;
5. приобретение навыков применения математических методов к решению прикладных задач защиты информации

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ УЧЕБНОГО ПЛАНА

Дисциплина относится к дисциплинам обязательной части блока Б1.
Требования к предварительной подготовке обучающегося: основные понятия и аксиомы информатики, методы, основные методы и приемы работы вычислительными сетями.
Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее: безопасность баз данных и операционных систем, стандартизация в сфере информационной безопасности, выпускная квалификационная работа.
Освоение дисциплины возможно с применением электронного обучения и дистанционных образовательных технологий.

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

ОПК-1. Способен применять естественно-научные и общеинженерные знания, методы математического анализа и моделирования, теоретического и экспериментального исследования в профессиональной деятельности
ОПК-1.1. Использует естественно-научные и общеинженерные знания математические методы и модели для теоретического и экспериментального исследования в профессиональной деятельности
ОПК-1.2. Осуществляет применение методов в экспериментальных исследованиях в профессиональной деятельности
ОПК-1.3. Анализирует полученные данные в теоретическом и экспериментальном исследовании объектов
ПК-1 Способен разрабатывать требования и проектировать программное обеспечение
ПК-1.1. Изучает требования к программному обеспечению
ПК-1.2. Осуществляет проектирование программного обеспечения
ПК-1.3. Формирует сборку модулей и компонент программного обеспечения

В результате освоения дисциплины обучающийся должен:

знать:

- связь теории кодирования и криптографии.
- криптографические свойства булевых функций и их применение в построении шифров современную историю криптографии;
- действующие стандарты шифрования данных;
- современные асимметричные криптосистемы;
- методы использования асимметричных шифров для решения проблемы распределения ключей, для создания электронной цифровой подписи и соответствующие стандарты
- различия между абсолютной и вычислительной стойкостью, свойства энтропии и их использование для оценки криптостойкости;
- принципы построения поточных и блочных симметричных шифров;
- современные стандарты шифрования
- основные математические методы защиты информации

уметь:

- различать характер воздействий на информацию и выбирать подходящие методы для решения задач профессиональной деятельности
- использовать теорию алгебраических систем в решении задач криптографии;
- решать линейные рекуррентные уравнения, анализировать свойства связанных с ними линейных рекуррентных последовательностей и делать вывод о пригодности характеристик в криптографических целях;
- исследовать булевы функции на наличие криптографических свойств;
- строить булевы функции с определенными криптографическими характеристиками
- реализовывать программно изученные алгоритмы шифрования и создания ЭЦП
- анализировать выбранные средства защиты данных на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности
- реализовывать алгоритмы защиты данных на основе математических методов

владеть/быть в состоянии продемонстрировать:

- математическими методами криптографии для решения прикладных задач.
- навыками анализа и обобщения передового опыта в сфере профессиональной деятельности
- методами и средствами научно-исследовательских работ по оценке защищенности информации в компьютерных системах
- методами и средствами анализа безопасности компьютерных систем
- навыками построения математических моделей элементов безопасности и разработки криптографических алгоритмов

4. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ / МОДУЛЯ

Общая трудоемкость дисциплины составляет 2 ЗЕТ (72_ часа/ов), в том числе в семестрах:

Семестр (для очной, очно-заочной)/ сессия/ курс (для заочной) №	Трудоемкость							РГР, курсовая работа, курсовой проект, контрольная работа (для заочной формы) (указывается вид работы)	Форма промежуточной аттестации
	Всего		Контактная работа			СРС	Контроль		
			час.						
	ЗЕТ	час.	Лк.	Пр.	Лаб.	час.	час.		
5/3	2	72	16		32	24			зачет

№	Наименование разделов и тем/ вид занятия	Семестр / сессия/ курс	Кол-во часов	Индикаторы достижения компетенций	Форма текущего контроля
1.	Тема 1. Предмет и задачи криптографии	5/3		ПК-1, ОПК-1	
	Лекция 1: Основные понятия: задачи, объект, предмет, методы криптографической безопасности. Требования к криптографическим системам защиты информации. Сведения из истории криптографии. Способы реализации криптографических методов.	5/3	2	ПК-1, ОПК-1	
	Лабораторная работа 1: Дешифрация шифротекста. Частотный криптоанализ.	5/3	4	ПК-1, ОПК-1	Защита отчета
	Лекция 2: Понятие и виды криптографических атак. Криптографический протокол. Криптографические методы защиты информации. Методы стеганографии. Классификация методов шифрования. Требования к современным шифрам.	5/3	2	ПК-1, ОПК-1	
	Лабораторная работа 2: Программная реализация шифра замены. Дешифрация шифротекста. Частотный криптоанализ.	5/3	4	ПК-1, ОПК-1	Защита отчета
	СРС	5/3	6	ПК-1, ОПК-1	
2.	Тема 2. Симметричные криптосистемы	5/3		ПК-1, ОПК-1	
	Лекция 3: Симметричные шифры. Поточные шифры. Блочные шифры.	5/3	2	ПК-1, ОПК-1	
	Лабораторная работа 3: Разработка ПО шифратора на основе генератора псевдослучайных чисел, основанного на свойствах М-последовательности.	5/3	4	ПК-1, ОПК-1	Защита отчета
	Лекция 4: Изучение криптосистемы DES. Распределение симметричных ключей. Разделение секрета.	5/3	2	ПК-1, ОПК-1	
	Лабораторная работа 4: Разработка ПО статистических тестов. Статистический анализ открытого текста, ключевой последовательности, шифрограммы.	5/3	4	ПК-1, ОПК-1	Защита отчета
	СРС	5/3	6	ПК-1, ОПК-1	
3.	Тема 3. Криптографические системы с открытым ключом.	5/3		ПК-1, ОПК-1	
	Лекция 5: Арифметика остатков. Односторонние функции. Алгоритм RSA. Криптосистема Эль-Гамаль.	5/3	2	ПК-1, ОПК-1	
	Лабораторная работа 5: Алгоритм RSA. Реализация арифметических операций. Библиотека BigInteger. Разложение чисел на множители методом ρ-эвристики Полларда.	5/3	4	ПК-1, ОПК-1	Защита отчета
	Лекция 6: Криптосистема Рабина. Схемы цифровой подписи: 1) RSA, 2) DSA, Хэш-функция	5/3	2	ПК-1, ОПК-1	
	Лабораторная работа 6: Хэш-функция. Проверка целостности сообщения. Электронная цифровая подпись. Хранение и проверка паролей.	5/3	4	ПК-1, ОПК-1	Защита отчета
	СРС	5/3	6	ПК-1, ОПК-1	
4.	Тема 4. Введение в криптографические протоколы..	5/3		ПК-1, ОПК-1	

	Лекция 7: Понятие криптографического протокола. Основные примеры. Связь стойкости протокола со стойкостью базовой криптографической системы. Классификация криптографических протоколов. Парольные схемы и протоколы ";рукопожатия";. Взаимосвязь между протоколами аутентификации и цифровой подписи. Протоколы сертификации ключей.	5/3	2	ПК-1, ОПК-1	
	Лабораторная работа 7: Изучение примитивных протоколов.	5/3	4	ПК-1, ОПК-1	Защита отчета
	Лекция 8: Протоколы предварительного распределения ключей. Протоколы выработки сеансовых ключей. Открытое распределение ключей Диффи-Хеллмана и его модификации. Вопросы организации сетей засекреченной связи. Доказательства с нулевым разглашением. Разделение секрета. Протоколы подбрасывания монеты. Построение протоколов с нулевым разглашением на основе NP-сложных задач.	5/3	2	ПК-1, ОПК-1	
	Лабораторная работа 8: Изучение криптосистемы Kerberos.	5/3	4	ПК-1, ОПК-1	Защита отчета
	СРС	5/3	6	ПК-1, ОПК-1	
	ИТОГО		72		

5. КОНТРОЛЬНЫЕ ВОПРОСЫ И ЗАДАНИЯ

5.1. Перечень контрольных вопросов и заданий для текущего контроля представлен в Фонде оценочных средств по данной дисциплине.

5.2. Перечень контрольных вопросов и заданий для промежуточной аттестации

5.2.1 Задания для проведения промежуточной аттестации в форме зачета могут включать:

- вопросы, требующие устного или письменного ответа:

1. Основные понятия, термины, определения. Криптология, криптография, криптоанализ, аутентификация, идентификация. Основные причины использования криптосистем. Симметричная криптосистема.
2. Исторические шифры. Шифр сдвига. Шифр замены. Полиалфавитный шифр. Шифр Виженера. Шифр Вернама. Недостатки исторических шифров. (Информационная стойкость).
3. Информационная стойкость криптографических систем Вычислительно защищенная криптосистема. Основные проблемы вычислительно защищенной криптосистемы. Абсолютно стойкая (совершенная) криптосистема.
4. К какому классу криптосистем - вычислительно защищенной или абсолютно стойкой относятся следующие криптосистемы: Шифр сдвига. Шифр замены. Шифр Виженера. Шифр Вернама ?
5. Понятие "абсолютной стойкости" в терминах теории вероятности. Теорема Шеннона: критерий абсолютной стойкости шифра. Интерпретация на примере шифра Вернама.
6. Энтропия случайной величины. Свойства энтропии. совместная энтропия двух случайных величин. Условная энтропия двух случайных величин. Неопределенность ключа.
7. Энтропия естественного языка. Расстояние единственности шифра.
8. Криптосистема с секретным ключом. Принцип Керкхоффа. Поточные и блочные

шифры.

9. Поточные шифры. Генератор ключевого потока. Свойства генератора ключевого потока. Генератор псевдослучайных чисел, основанный на использовании алгебраических свойств М-последовательностей

10. Статистические тесты генераторов ключевого потока.

11. Блочные шифры. Алгоритм DES. Перестановки. Раунды. Алгоритм Фейстеля при шифровании и дешифровании.

12. Сравнение блочных и поточных шифров. Методы организации процедуры исправления ошибок.

13. Статичный ключ. Эфемерный ключ. Распределение ключей. Основные пути решения проблемы распределения ключей. (физические методы, Протоколы с секретным ключом, Протоколы с открытым ключом, современные физические методы).

14. Разделение секрета. Схема порогового разделения секрета. (T, W) - пороговая схема Шамира.

15. Протоколы распределения секретных ключей. Основные цели протокола распределения ключей. Протокол Барроуза.

16. Протоколы распределения секретных ключей. Основные цели протокола распределения ключей. Протокол Нидхейма-Шредера

17. Протоколы распределения секретных ключей. Основные цели протокола распределения ключей. Протокол Отвэй-Риса.

18. Протоколы распределения секретных ключей. Основные цели протокола распределения ключей. Цербер

19. Арифметика остатков. Сравнение по модулю. Решение уравнения $ax = b \pmod N$.

20. Функция Эйлера. Мультипликативные обратные по модулю N. Теорема Лагранжа. Малая теорема Ферма. Применение в криптографии.

21. Алгоритм Евклида. Китайская теорема об остатках. Расширенный алгоритм Евклида. Применение в криптографии.

22. Криптосистема с открытым ключом. Криптографическая односторонняя функция. Важнейшие криптографические односторонние функции.

23. Оценка сложности задач. Сложность алгоритма: Полиноминальная, экспоненциальная, субэкспоненциальная Оракул. Сравнительный анализ сложности криптографических алгоритмов (без доказательства).

24. Алгоритм RSA. Шифрование в RSA. Дешифрование в RSA. Доказательство алгоритма.

25. Алгоритм RSA. Задача криптоаналитика. Криптостойкость RSA

26. Криптосистема Эль-Гамаль. Параметры домена. Шифрование. Дешифрование.

27. Криптосистема Рабина. Алгоритм. Шифрование. Дешифрование.

28. Простые числа. Важность проблемы тестирования простых чисел. Пробное деление. Вероятностный подход при определении простого числа. Тест Ферма. Тест Миллера ? Рабина.

29. Распределение ключей Диффи ? Хеллмана. Алгоритм. Стойкость. Атака человек посередине. Необходимость использования цифровой подписи.

30. Алгоритмом цифровой подписи RSA

31. Криптографическая Хэш-функция. Свойства криптографической хэш-функции.Свойство односторонности Защищенность от повторений, защищенностью от

вторых прообразов.

32. Алгоритмом цифровой подписи DSA
33. Отечественный стандарт цифровой подписи ГОСТ Р 34.10-94
34. Квантовая криптография
35. Передача секретных ключей по радиоканалу

- тесты, проводимые в письменной или электронной форме.

Вопрос 1. Что такое шифрование?

а) способ изменения сообщения или другого документа, обеспечивающее искажение его содержимого +

б) совокупность тем или иным способом структурированных данных и комплексом аппаратно-программных средств

в) удобная среда для вычисления конечного пользователя

Вопрос 2. Что такое шифрование?

а) преобразовательный процесс исходного текста в зашифрованный+

б) упорядоченный набор из элементов алфавита

в) нет правильного ответа

5.2.2 Оценивание уровня сформированности индикаторов компетенций у обучающихся на соответствие их подготовки ожидаемым результатам, описание их показателей, критериев и шкал оценивания в процессе проведения промежуточной аттестации представлено в Фонде оценочных средств по данной дисциплине.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ / МОДУЛЯ

6.1. Учебно-методическое обеспечение

Библиографическое описание по ГОСТ	**Кол-во экземпляров в НБ ВоГУ**
1	**2**
Рекомендуемая литература	
1. Артемов, А. В. Информационная безопасность [Электронный ресурс]: курс лекций/ А. В. Артемов. - Орел: МАБИВ, 2014. - 257 с.: табл., схем. - Режим доступа: http://biblioclub.ru/index.php?page=book&id=428605	ЭБС «Университетская библиотека онлайн»
2. Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации [Электронный ресурс]: учебное пособие/ Ю. Н. Загинайлов. - Москва; Берлин: Директ-Медиа, 2015. - 253 с.: ил. - Режим доступа: http://biblioclub.ru/index.php?page=book&id=276557	ЭБС «Университетская библиотека онлайн»
3. Нестеров, С. А. Основы информационной безопасности [Электронный ресурс]: учебное пособие/ С. А. Нестеров. - Санкт-Петербург: СПбПУ, 2014. - 322 с.: схем., табл., ил. - Режим доступа: http://biblioclub.ru/index.php?page=book&id=363040	ЭБС «Университетская библиотека онлайн»
4. Галатенко, В. А. Основы информационной безопасности: курс лекций: учебное пособие для вузов/ В. А. Галатенко; под ред. В. Б. Бетелина. - Москва: ИНТУИТ, 2004. - 260 с.	15
5. Галатенко, В. А. Стандарты информационной безопасности: курс	5

лекций: для вузов/ В. А. Галатенко; под ред. В. Б. Бетелина. - Москва: ИНТУИТ, 2004. - 322 с.	
6. Завгородний, В. И. Комплексная защита информации в компьютерных системах: учебное пособие для вузов/ В. И. Завгородний. - Москва: Логос, 2001. - 263 с.	5
7. Ложников, П. С. Обеспечение безопасности сетевой инфраструктуры на основе операционных систем Microsoft [Электронный ресурс]: практикум/ П. С. Ложников, Е. М. Михайлов. - Москва: ИНТУИТ, 2008. - 246 с. - Режим доступа: http://biblioclub.ru/index.php?page=book&id=233194	ЭБС «Университетская библиотека онлайн»
8. Мельников, В. П. Информационная безопасность и защита информации: учебное пособие для вузов/ В. П. Мельников, С. А. Клейменов, А. М. Петраков; под ред. С. А. Клейменова. - 3-е изд., стер. - Москва: Academia, 2008. - 330, [1] с. ил.	5
9. Петренко, В. И. Теоретические основы защиты информации [Электронный ресурс]: учебное пособие/ В. И. Петренко. - Ставрополь: СКФУ, 2015. - 222 с. - Режим доступа: http://biblioclub.ru/index.php?page=book&id=458204	ЭБС «Университетская библиотека онлайн»
10. Прохорова, О. В. Информационная безопасность и защита информации [Электронный ресурс]: учебник/ О. В. Прохорова. - Самара: СГАСУ, 2014. - 113 с.: табл., схем., ил. - Режим доступа: http://biblioclub.ru/index.php?page=book&id=438331	ЭБС «Университетская библиотека онлайн»
11. Романец, Ю. В. Защита информации в компьютерных системах и сетях/ Ю. В. Романец, П. А. Тимофеев; В. Ф. Шаньгин. - 2-е изд., перераб. и доп. - Москва: Радио и связь, 2001. - 376 с.: ил.	4
12. Романов, О. А. Организационное обеспечение информационной безопасности: учебник для вузов/ О. А. Романов, С. А. Бабин, С. Г. Жданов. - Москва: Academia, 2008. - 188, [1] с.	5
13. Скрипник, Д. А. Общие вопросы технической защиты информации Электронный ресурс]: курс/ Д. А. Скрипник. - 2-е изд., испр. - Москва: ИНТУИТ, 2016. - 425 с.: ил. - Режим доступа: http://biblioclub.ru/index.php?page=book&id=429070	ЭБС «Университетская библиотека онлайн»
14. Суконщиков, А. А. Методы и средства защиты компьютерной информации: учебное пособие по специальности "Управление и информатика в технических системах"/ А. А. Суконщиков, Е. Н. Давыдова. - Вологда: ВоГТУ, 2008. - 132 с.: ил. - Режим доступа: http://www.library.vstu.edu.ru/biblio/sukonshikov/book1/2008_sukonshikov_sash_inf.pdf	40 ЭБ ВоГУ
15. Технологии защиты информации в компьютерных сетях [Электронный ресурс]/ Н. А. Руденков, А. В. Пролетарский, Е. В. Смирнова, А. М. Суровов. - 2-е изд., испр. - Москва: ИНТУИТ, 2016. - 369 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=428820	ЭБС «Университет-ская библиотека онлайн»
16. Хорев, П. Б. Методы и средства защиты информации в компьютерных системах: учебное пособие для вузов/ П. Б. Хорев. - Москва: Academia, 2005. - 254, [1] с.: ил.	20
17. Цирлов, В. Л. Основы информационной безопасности: краткий курс: [учебник для вузов]/ В. Л. Цирлов. - Ростов-на-Дону: Феникс, 2008. - 253,	5

[1] с.	
18. Щербаков, А. Современная компьютерная безопасность. Теоретические основы. Практические аспекты [Электронный ресурс]: учебное пособие/ А. Щербаков. - Москва: Книжный мир, 2009. - 352 с. - Режим доступа: http://biblioclub.ru/index.php?page=book&id=89798	ЭБС «Университетская библиотека онлайн»
19. Защита информации: методические указания к лабораторным работам: ЭЭФ: направления подготовки бакалавриата: 27.03.04 - Управление в технических системах, 09.03.01 - Информатика и вычислительная техника, 09.03.04 - Программная инженерия : профили подготовки: "Управление и информатика в технических системах", "Программное обеспечение средств вычислительной техники и автоматизированных систем", "Разработка программно-информационных систем"/ сост. Е. Н. Давыдова. - Вологда: ВоГУ, 2014. - 31 с.: ил. - Режим доступа: http://www.library.vstu.edu.ru/biblio/davydova/book10/2014_davydova_zash_inf.pdf	10 ЭБ ВоГУ
20. Методы и средства защиты компьютерной информации: методические указания к практической работе № 4 "Применение механизмов QoS в системах защиты информации": ЭЭФ, ФЗДО: специальности: 220201, 230101/ [сост.: Е. Н. Давыдова, А. А. Суконщиков]. - Вологда: ВоГТУ, 2009. - 15 с.: ил. - Режим доступа: http://www.library.vstu.edu.ru/biblio/davydova/book7/2009_davydova_4.pdf	29 ЭБ ВоГУ
21. Методы и средства защиты компьютерной информации: методические указания к лабораторной работе №5 "Изучение алгоритмов шифрования": ЭЭФ, ФЗДО: специальности: 220201, 230101/ [сост.: Суконщиков А. А., Давыдова Е. Н.]. - Вологда: ВоГТУ, 2009. - 11, [1] с.: ил. - Режим доступа: http://www.library.vstu.edu.ru/biblio/sukonshikov/book4/2009_sukonshikov_sash_inf_lr5.pdf	14 ЭБ ВоГУ

6.2. Информационное обеспечение

1. Основы информационной безопасности https://www.intuit.ru/studies/courses/10/10/info
2. Введение в защиту информации от внутренних ИТ-угроз https://www.intuit.ru/studies/courses/1013/172/info
3. Доступ к учебно-методическому комплексу кафедры АВТ http://atpp.vstu.edu.ru/umk/
4. Доступ к учебно-методическому порталу ВоГУ https://do.vogu35.ru/

6.3 Программное обеспечение

1. Windows 10
2. LibreOffice

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ / МОДУЛЯ

№№ п/п	Перечень основного оборудования
1	**2**
1.	*Персональный компьютер*
2.	*Проектор Epson EB-X10 (1 шт.)*

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 20 / 20 учебном году на заседании кафедры Автоматики и вычислительной техники

Протокол от ____ _____ 20__ г. № ___
Зав. кафедрой

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в / учебном году на заседании кафедры

_____

Протокол от _20_ г. № _ Зав. кафедрой _

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в / учебном году на заседании кафедры

_____

Протокол от _20_ г. № _ Зав. кафедрой _

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ,
ВНОСИМЫЕ В РАБОЧУЮ ПРОГРАММУ ДИСЦИПЛИНЫ

№ п/п	Содержание изменения	Основание для внесения изменений	Автор рабочей программы дисциплины, ответственный за внесение изменений	Зав.кафедрой
1.		протокол от «__» _20__г № _	ФИО, подпись	ФИО, подпись
2.		протокол от «__» _20__г № _	ФИО, подпись	ФИО, подпись
3.		протокол от «__» _20__г № _	ФИО, подпись	ФИО, подпись