МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»
(РУТ (МИИТ)

Рабочая программа дисциплины (модуля),
как компонент образовательной программы
высшего образования - программы бакалавриата
по направлению подготовки
10.03.01 Информационная безопасность,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Криптографическая защита информации

Направление подготовки: 10.03.01 Информационная безопасность

Направленность (профиль): Безопасность компьютерных систем

Форма обучения: Очная

1. Общие сведения о дисциплине (модуле).

Целью освоения учебной дисциплины «Криптографическая защита информации» является формирование профессиональных компетенций по основным разделам дисциплины.

Задачами дисциплины являются:

- изучение основных методов и средств криптографической защиты информации, стандартов в этой области;
- получение представления о математических методах криптографической защиты информации;
- студенты должны научиться применять современные методы и средства криптографической защиты информации на практике.

2. Планируемые результаты обучения по дисциплине (модулю).

Перечень формируемых результатов освоения образовательной программы (компетенций) в результате обучения по дисциплине (модулю):

ОПК-3 - Способен использовать необходимые математические методы для решения задач профессиональной деятельности;

ОПК-9 - Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности ;

ПК-1 - способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации .

Обучение по дисциплине (модулю) предполагает, что по его результатам обучающийся будет:

Знать:

- математические методы и основополагающие документы в области криптографической защищенности компьютерных систем (КС) и сетей;
- международные и национальные стандарты по оценке безопасности в области информационных технологий;
- порядок тестирования функций программных и программно-аппаратных (в том числе криптографических) средств защиты информации.

Уметь:

- оценивать уровень безопасности КС и сетей;
- применять стандарты и другие нормативные документы по информационной безопасности для оценки защищенности КС;

- проводить контроль показателей и процесса функционирования программных и программно- аппаратных (в том числе криптографических) средств защиты информации.

Владеть:

- навыками работы по установке, настройке и обслуживанию программных, программно-аппаратных и технических средств защиты информации;
- навыками поддержания бесперебойной работы программных и программно- аппаратных (в том числе криптографических) средств защиты информации в ИТКС;
- навыками использования средств криптографической и технической защиты информации для решения задач профессиональной деятельности.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 8 з.е. (288 академических часа(ов).

3.2. Объем дисциплины (модуля) в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Тип учебных занятий	Количество часов		
	Всего	Семестр	
		№5	№6
Контактная работа при проведении учебных занятий (всего):	112	48	64
В том числе:			
Занятия лекционного типа	64	32	32
Занятия семинарского типа	48	16	32

3.3. Объем дисциплины (модуля) в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении промежуточной аттестации составляет 176 академических часа (ов).

3.4. При обучении по индивидуальному учебному плану, в том числе при ускоренном обучении, объем дисциплины (модуля) может быть реализован полностью в форме самостоятельной работы обучающихся, а также в форме

контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении промежуточной аттестации.

4. Содержание дисциплины (модуля).

4.1. Занятия лекционного типа.

№ п/п	Тематика лекционных занятий / краткое содержание
1	5 СЕМЕСТР ЗАЩИТА ИНФОРМАЦИИ Рассматриваемые вопросы: - требования ФСТЭК по защите информации; - рекомендации по технической защите данных; - классы средств защиты данных.
2	ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ Рассматриваемые вопросы: - меры по обеспечению информационной безопасности; - документы ФСТЭК по ИБ; - сертифицированные средства ИБ ФСТЭК.
3	ЗАЩИТА КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ Рассматриваемые вопросы: - порядок обеспечения информационной безопасности; - криптографическая защита информации.
4	КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ Рассматриваемые вопросы: - методы защиты виды, классификация; - шифрование, стенография, кодирование, сжатие и др..
5	КРИПТОГРАФИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ Рассматриваемые вопросы: - средства криптографической защиты информации (СКЗИ); - сертифицированные криптографические средства защиты информации в России.
6	ЭЛЕМЕНТЫ ТЕОРИИ ЧИСЕЛ Рассматриваемые вопросы: - алгоритм Евклида, соотношение Безу; - Диофантовы линейные уравнения; - теорема Ферма, функция и теорема Эйлера; - квадратичные вычеты, символы Лежандра и Якоби.
7	ТЕСТИРОВАНИЕ ЧИСЕЛ НА ПРОСТОТУ И ПОСТРОЕНИЕ Рассматриваемые вопросы: - элементарные методы проверки простоты чисел; - алгоритмы Конягина-Померанса, Миллера; - вероятностные тесты на простоту и детерминированный полиномиальный алгоритм проверки простоты чисел.
8	ФАКТОРИЗАЦИЯ ЦЕЛЫХ ЧИСЕЛ С ЭКСПОНЕНЦИАЛЬНОЙ СЛОЖНОСТЬЮ Рассматриваемые вопросы: - методы Ферма, Полларда, Шермана-Лемана,

№ п/п	Тематика лекционных занятий / краткое содержание
	- алгоритмы Ленстры и Полларда-Штрассена; - (P +1)-метод Уильямса и его обобщения.
9	ФАКТОРИЗАЦИЯ ЦЕЛЫХ ЧИСЕЛ С СУБЭКСПОНЕНЦИАЛЬНОЙ СЛОЖНОСТЬЮ Рассматриваемые вопросы: - методы Диксона, Шнорра-Ленстры, Ленстры-Померанса; - алгоритм Бриллхарта-Моррисона; - алгоритмы решета числового поля.
10	АЛГЕБРАИЧЕСКИЕ СТРУКТУРЫ: ГРУППЫ, КОЛЬЦА, ПОЛЯ Рассматриваемые вопросы: - группы, морфизмы групп, кольца, поля; - поля Галуа или конечные поля; - задача дискретного логарифмирования в конечных полях; - кольцо многочленов.
11	ПРИМЕНЕНИЕ КРИВЫХ ДЛЯ ПРОВЕРКИ ПРОСТОТЫ И ФАКТОРИЗАЦИИ Рассматриваемые вопросы: - эллиптические кривые и их свойства; - алгоритм Ленстры для факторизации целых чисел с помощью эллиптических кривых; - вычисление порядка группы точек эллиптической кривой над конечным полем; - тестирование чисел на простоту с помощью эллиптических кривых.
12	АЛГОРИТМЫ ДИСКРЕТНОГО ЛОГАРИФМИРОВАНИЯ Рассматриваемые вопросы: - детерминированные методы; - дискретное логарифмирование в простых полях, в полях Галуа; решето числового поля; - частное Ферма и дискретное логарифмирование по составному модулю.
13	ФАКТОРИЗАЦИЯ МНОГОЧЛЕНОВ НАД КОНЕЧНЫМИ ПОЛЯМИ Рассматриваемые вопросы: - вероятностный алгоритм решения алгебраических уравнений в конечных полях; - решение квадратных уравнений; - вероятностный алгоритм проверки неприводимости многочленов над конечными полями.
14	ПРИВЕДЕННЫЕ БАЗИСЫ РЕШЕТОК И ИХ ПРИЛОЖЕНИЯ Рассматриваемые вопросы: - решетки и базисы; - LLL-приведенный базис и его свойства; - алгоритм Фергюсона-Форкейда.
15	Рассматриваемые вопросы: Рассматриваемые вопросы: - LLL-алгоритм факторизации; - факторизация многочленов с использованием приближенных вычислений.
16	ДИСКРЕТНОЕ ПРЕОБРАЗОВАНИЕ ФУРЬЕ Рассматриваемые вопросы: - вычисление дискретного преобразования Фурье; - применение дискретного преобразования Фурье в алгоритме Полларда-Штрассена.
17	6 СЕМЕСТР ЦЕЛОЧИСЛЕННАЯ АРИФМЕТИКА МНОГОКРАТНОЙ ТОЧНОСТИ Рассматриваемые вопросы: - основные операции; - алгоритмы модулярной арифметики.

№ п/п	Тематика лекционных занятий / краткое содержание
18	СИСТЕМЫ ЛИНЕЙНЫХ УРАВНЕНИЙ НАД КОНЕЧНЫМИ ПОЛЯМИ Рассматриваемые вопросы: - решение систем линейных уравнений в целых числах; - гауссово и структурированное гауссово исключение; - алгоритмы Ланцоша и Видемана.
19	ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ Рассматриваемые вопросы: - понятие эллиптической кривой над полем; - порядок эллиптической кривой; - применение эллиптических кривых в криптографии.
20	КРИПТОГРАФИЧЕСКИЕ КЛЮЧИ Рассматриваемые вопросы: - управление криптографическими ключами; - генерация ключей; - хранение ключей; - распределение ключей.
21	КРИПТОГРАФИЧЕСКИЕ ПРИМИТИВЫ Рассматриваемые вопросы: - свойства примитивов, основные примитивы, объединение примитивов; - свойства безопасности.
22	КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ Рассматриваемые вопросы: - отличия протоколов от криптосистем; - виды атак на криптографические протоколы; - базовые протоколы; - стандартные протоколы.
23	КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ ЭЛЕКТРОННЫХ ПЛАТЕЖЕЙ Рассматриваемые вопросы: - электронная подпись; - протоколы электронных платежей, другие виды протоколов.
24	СИММЕТРИЧНЫЕ И АССИМЕТРИЧНЫЕ КРИПТОСИСТЕМЫ 1 Рассматриваемые вопросы: - стандарты шифрования данных (алгоритм шифрования данных DES, Triple DES, AES, алгоритм Ривеста); - Российский стандарт крипто- и имитозащиты сообщений.
25	СИММЕТРИЧНЫЕ И АССИМЕТРИЧНЫЕ КРИПТОСИСТЕМЫ 2 Рассматриваемые вопросы: - концепция криптосистемы с открытым ключом; - криптосистема шифрования данных RSA, схемы шифрования Полига-Хеллмана, Эль Гамаля, комбинированный метод шифрования.
26	ХЭШ-ФУНКЦИИ Рассматриваемые вопросы: - виды; - хэш-функции - использование в ЭП, стандарты хэш-функций.

№ п/п	Тематика лекционных занятий / краткое содержание
27	ЭЛЕКТРОННАЯ ПОДПИСЬ Рассматриваемые вопросы: - проблема аутентификации данных; - подписи с дополнительными функциональными свойствами.
28	АЛГОРИТМЫ ЭП Рассматриваемые вопросы: - алгоритмы электронной подписи (назначение и виды, классификация, подделка ЭП); - слепая ЭП, быстрая, неоспоримая.
29	Рассматриваемые вопросы: Рассматриваемые вопросы: - формальные методы доказательства правильности программ и их спецификаций; - методы и средства анализа безопасности ПО; - контрольно-испытательные и логико-аналитические методы.
30	БЕЗОПАСНОСТЬ ТЕХНИЧЕСКИХ СРЕДСТВ КОМПЬЮТЕРНЫХ СИСТЕМ Рассматриваемые вопросы: - требования к техническим средствам; - анализ безопасности технических средств КС; - подходы к оценке информационной безопасности.
31	ОСНОВНЫЕ МЕТОДЫ ДЛЯ РЕШЕНИЯ ПРОБЛЕМЫ ОПРЕДЕЛЕНИЯ УРОВНЯ ЗАЩИЩЕННОСТИ КС Рассматриваемые вопросы: - структура критериев оценки соответствия уровня защищенности; - показатели уязвимости; - использование эмпирического, теоретического и теоретико-эмпирического методов.
32	ПРОЕКТИРОВАНИЕ СИСТЕМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ Рассматриваемые вопросы: - принципы построения систем защиты конфиденциальной информации; - основы политики безопасности (понятие политики безопасности, реализация политики безопасности, модели безопасности); - основные этапы проектирования.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	5 СЕМЕСТР КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ В результате работы студентом будут исследованы и проанализированы криптографические методы и средства защиты информации, подготовлен отчет.
2	ФАКТОРИЗАЦИЯ ЦЕЛЫХ ЧИСЕЛ С ЭКСПОНЕНЦИАЛЬНОЙ СЛОЖНОСТЬЮ Результат работы – реализация алгоритмов Ленстры и Полларда-Штрассена.

№ п/п	Тематика практических занятий/краткое содержание
3	ФАКТОРИЗАЦИЯ ЦЕЛЫХ ЧИСЕЛ С СУБЭКСПОНЕНЦИАЛЬНОЙ СЛОЖНОСТЬЮ Результат работы – реализация алгоритмов Бриллхарта-Моррисона и алгоритмов решета числового поля.
4	Результат работы – реализация алгоритмов Бриллхарта-Моррисона и алгоритмов решета числового поля. Результат работы – отчет с решением задач по теме «Дискретное логарифмирование в простых полях и в полях Галуа».
5	ВЕРОЯТНОСТНЫЙ АЛГОРИТМ РЕШЕНИЯ АЛГЕБРАИЧЕСКИХ УРАВНЕНИЙ Результат работы – реализация вероятностного алгоритма проверки неприводимости многочленов над конечными полями.
6	РЕШЕТКИ И БАЗИСЫ Результат работы – реализация алгоритма Фергюсона-Форкейда.
7	ФАКТОРИЗАЦИЯ МНОГОЧЛЕНОВ Результат работы – решение задач по теме «Факторизация многочленов с использованием приближенных вычислений».
8	ПРЕОБРАЗОВАНИЕ ФУРЬЕ Результат работы – отчет с исследованием применения дискретного преобразования Фурье в алгоритме Полларда-Штрассена.
9	6 СЕМЕСТР АЛГЕБРАИЧЕСКИЕ СТРУКТУРЫ: ГРУППЫ, КОЛЬЦА, ПОЛЯ Результат работы – получение практических навыков решения задач.
10	ЦЕЛОЧИСЛЕННАЯ АРИФМЕТИКА МНОГОКРАТНОЙ ТОЧНОСТИ Результат работы – отчет с результатами проведенного анализа алгоритмов модулярной арифметики.
11	РЕШЕНИЕ СИСТЕМ ЛИНЕЙНЫХ УРАВНЕНИЙ НАД КОНЕЧНЫМИ ПОЛЯМИ Результат работы – реализация алгоритмов Ланцоша и Видемана.
12	ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ И ИХ СВОЙСТВА Результат работы – отчет с результатами тестирования чисел на простоту с помощью эллиптических кривых.
13	ХРАНЕНИЕ КЛЮЧЕЙ Результат работы – отчет с результатами исследования методов и средств хранения ключей.
14	Результат работы – отчет с результатами исследования методов и средств хранения ключей. Результат работы – отчет, где представлены схемы и алгоритмы генерации сеансового ключа.
15	Результат работы – отчет, где представлены схемы и алгоритмы генерации сеансового ключа. Результат работы – отлаженная программа, реализующая протокол привязки к биту (протокол Блюма - схема Блюма-Микали).
16	ЭЛЕКТРОННАЯ ПОДПИСЬ Студент получит навыки применения соответствующих стандартов, будет знать процессы формирования и проверки ЭП, особенности использования функции хэширования в схемах ЭП.

№ п/п	Тематика практических занятий/краткое содержание
17	ФУНКЦИЯ ХЭШИРОВАНИЯ Студент получит навыки применения соответствующих стандартов, будет знать особенности использования функции хэширования в схемах ЭП.
18	ИЗУЧЕНИЕ МЕТОДОВ ШИФРОВАНИЯ Результат работы – зашифрованное сообщение с использованием традиционных методов шифрования (предварительно выбрав ключ).
19	ИССЛЕДОВАНИЕ И ПРОГРАММНАЯ РЕАЛИЗАЦИЯ МЕТОДОВ ШИФРОВАНИЯ Результатом работы является отлаженная программа, реализующая предложенный студентом алгоритм шифрования.
20	СОВРЕМЕННЫЕ СИММЕТРИЧНЫЕ И АССИМЕТРИЧНЫЕ КРИПТОСИСТЕМЫ Результатом работы является отлаженная программа, реализующая заданный студенту криптографический алгоритм.
21	ОБЩИЕ КРИТЕРИИ ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ Результат работы – навыки практического применения соответствующего стандарта.
22	ОЦЕНКА БЕЗОПАСНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ Результат работы – список угроз и мер по разработке безопасного ПО, согласно ГОСТ Р 58412-2019.
23	ЗАЩИТА СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ И АВТОМАТИЗИРОВАННЫХ СИСТЕМ Результат работы - получение навыков практического применения Руководящего документа.
24	РАЗРАБОТКА СИСТЕМЫ ИНФОРМАЦИОННОЙ ЗАШИТЫ ОБЪЕКТА ИНФОРМАТИЗАЦИИ В результате выполнения работы студентом будет подготовлен отчет с описанием системы защиты информации.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Изучение дополнительной литературы
2	Работа с лекционным материалом
3	Подготовка к практическим занятиям
4	Выполнение курсовой работы.
5	Подготовка к промежуточной аттестации.
6	Подготовка к текущему контролю.

4.4. Примерный перечень тем курсовых работ

- Реализация алгоритма Ривеста.

- Реализация алгоритма DES – режим сцепления блоков в CBC шифре.

- Реализация алгоритма DES – режим работы ECB (электронный блокнот).

- Реализация алгоритма DES – режим работы CFB – обратная связь по шифротексту.

- Реализация алгоритма DES – OFB – обратная связь по выходу.

- Алгоритм федерального стандарта x9.9.

- Алгоритм криптографического преобразования – общий.

- Алгоритм криптографического преобразования в режиме простой замены.

- Алгоритм криптографического преобразования в режиме гаммирования с обратной связью

- Алгоритм криптографического преобразования в режиме имитовставки.

- Алгоритм, основанный на схеме шифрования Эль Гамаля.

- Алгоритм, основанный на комбинированном методе шифрования

- Открытое распределение ключей Диффи-Хеллмана

- Алгоритм электронной подписи RSA.

- Алгоритм электронной подписи DSA.

- Отечественный стандарт электронной подписи.

- Алгоритм цифровой подписи с дополнительными функциями по схеме «слепой подписи».

- Алгоритм цифровой подписи с дополнительными функциями по схеме «неоспоримой подписи».

5. Перечень изданий, которые рекомендуется использовать при освоении дисциплины (модуля).

№ п/п	Библиографическое описание	Место доступа
1	Вострецова Е.В. Основы информационной безопасности: учебное пособие для студентов	https://elar.urfu.ru/bitstream/10995/73899/3/978-5-7996-2677-8_2019.pdf,(дата обращения: 16.05.2024). - Текст:электронный.

	вузов. Екатеринбург: Изд-во Урал. ун-та, 2019.- 204 с. - ISBN 978-5-7996-2677-8.	
2	Казарин О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва: Издательство Юрайт, 2022. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2.	https://book-pc.ru/bezopasnost/1882-programmno-apparatnye-sredstva-zaschity-informacii.html,(дата обращения: 16.05.2024). - Текст:электронный.
3	Голиков А. М. Защита информации в инфокоммуникационных системах и сетях: учебное пособие / А. М. Голиков. — Москва: ТУСУР, 2015. — 284 с. // Лань: электронно-библиотечная система.	https://e.lanbook.com/book/110336,(дата обращения: 03.05.2024). — Режим доступа: для авториз. пользователей. — Текст: электронный
4	Нестеров С. А. Основы информационной безопасности: учебное пособие / С. А. Нестеров. — 5-е изд., стер. — Санкт-Петербург: Лань, 2022. — 324 с. — ISBN 978-5-8114-4067-2.	https://www.litres.ru/book/s-a-nesterov/osnovy-informacionnoy-bezopasnosti-66007377/,(дата обращения: 16.05.2024). — Режим доступа: для авториз. пользователей. Текст:электронный.
5	Лось А. Б., Нестеренко, А. Ю., Рожков, М. И. Криптографические методы защиты информации для изучающих компьютерную	https://azon.market/image/catalog/v_1/product/pdf/378/3777079.pdf, (дата обращения: 17.05.2024). — Режим доступа: для авториз. пользователей. — Текст: электронный

	безопасность: учебник для академического бакалавриата / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — М.: Издательство Юрайт, 2019. — 473 с. — (Серия: Бакалавр. Академический курс). - ISBN 978-5-534-12474-3.	

6. Перечень современных профессиональных баз данных и информационных справочных систем, которые могут использоваться при освоении дисциплины (модуля).

Форум специалистов по информационным технологиям http://citforum.ru/

Интернет-университет информационных технологий http://www.intuit.ru/

Поисковые системы: Yandex, Google, Mail.

Официальный сайт РУТ (МИИТ) (https://www.miit.ru/).

Научно-техническая библиотека РУТ (МИИТ) (http:/library.miit.ru).

Образовательная платформа «Юрайт» (https://urait.ru/).

Общие информационные, справочные и поисковые системы «Консультант Плюс», «Гарант».

Электронно-библиотечная система издательства «Лань» (http://e.lanbook.com/).

7. Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства, необходимого для освоения дисциплины (модуля).

Microsoft Internet Explorer (или другой браузер).

Операционная система Microsoft Windows.

Microsoft Office.

Специализированное программное обеспечение не требуется.

8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю).

Учебные аудитории для проведения учебных занятий, оснащенные компьютерной техникой и наборами демонстрационного оборудования.

9. Форма промежуточной аттестации:

Зачет в 5 семестре.
Курсовая работа в 6 семестре.
Экзамен в 6 семестре.

10. Оценочные материалы.

Оценочные материалы, применяемые при проведении промежуточной аттестации, разрабатываются в соответствии с локальным нормативным актом РУТ (МИИТ).

Авторы:

доцент, к.н. кафедры
«Вычислительные системы, сети и
информационная безопасность» Я.М. Голдовский

Согласовано:

Заведующий кафедрой ВССиИБ Б.В. Желенков

Председатель учебно-методической
комиссии Н.А. Андриянова