МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ

Заведующий кафедрой
функционального анализа
и операторных уравнений

Каменский М.И.
20.03.2025 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.О.36 Защита информации

1. Код и наименование направления подготовки: 01.03.04 Прикладная математика

2. Профиль подготовки: Применение математических методов к решению инженерных и экономических задач

3. Квалификация выпускника: бакалавр
4. Форма обучения: очная

5. Кафедра, отвечающая за реализацию дисциплины: функционального анализа и операторных уравнений

6. Составители программы: Завгородний Михаил Григорьевич, канд. физ-мат. наук, доцент

7. Рекомендована: НМС математического факультета, протокол № 0500-03 от 18.03.2025 г.

8. Учебный год: 2028-2029 **Семестр(ы):** 8

9.**Цели и задачи учебной дисциплины:**

Цель курса - ознакомление студентов с тенденцией развития информационной безопасности, с моделями возможных угроз, терминологией и основными понятиями теории безопасности информации, а также с нормативными документами России по данному вопросу и правилами получения соответствующих лицензий.

Основными задачами изучения дисциплины являются:

- получение студентами знаний по существующим угрозам безопасности информации, подбору и применению современных методов и способов защиты информации;

- формирование навыков, необходимых студентам по защите информации и администраторам локальных сетей.

10. Место учебной дисциплины в структуре ООП:

Дисциплина относится к обязательной части блока 1.Дисциплина(модули). Для изучения и освоения дисциплины нужны знания из предшествующих курсов: Программные аппаратные средства информатики, Теория графов и математическая логика, Программирование для ЭВМ, Операционные системы и сети, Базы данных, Математическое моделирование, Алгоритмы дискретной математики. Знания и умения, приобретенные студентами в результате изучения дисциплины, будут использоваться при выполнении курсовых и дипломных работ, связанных с математическим моделированием в области защиты информации.

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников):

Код	Название компетенции	Код(ы)	Индикатор(ы)	Планируемые результаты обучения
ОПК-4	Способен разрабатывать алгоритмы и компьютерные программы, пригодные для практического применения	ОПК-4.1	Использует основные принципы алгоритмизации задач в рамках профессиональной деятельности и разработки компьютерных программ	Знать: основные принципы проектирования, разработки программных продуктов Уметь: выявлять критерии оценивания программных продуктов и направления информационных угроз Владеть: навыками разработки и реализации программных продуктов, а также навыками организации аппаратно-программной защиты информации
		ОПК-4.2	Проводит тестирование и отладку компьютерных программ с целью апробации разработанных моделей и алгоритмов	Знать: основные принципы работы систем управления базами данных и телекоммуникационных сетей с учетом требований информационной безопасности Уметь: применять требования информационной безопасности при работе с системами управления базами данных и телекоммуникационными сетями Владеть: навыками организации безопасной работы систем управления базами данных и телекоммуникационных сетей
ОПК-1	Способен применять знание фундаментальной математики и естественно-научных дисциплин при решении задач в	ОПК-1.1	Обладает базовыми знаниями, полученными в области математических и (или) естественных наук	Знать: основные проблемы защиты информации и направления угроз информационной безопасности, а также методы и средства реализации этих угроз Уметь: применять знания, полученными в области математических и естественных наук, для решения задач защиты информации

	области естественных наук и инженерной практике			Владеть: навыками создания систем защиты информации
		ОПК-1.2	Умеет использовать базовые знания в области математических и (или) естественных наук в профессиональной деятельности	Знать: правовые нормы и основные принципы сбора, обработки, хранения и передачи информации Уметь: работать с информационно справочными системами Владеть: навыками работы с системами управления базами данных и телекоммуникационными сетями
		ОПК-1.3	Имеет навыки выбора методов решения задач профессиональной деятельности на основе теоретических знаний	Знать: основные методы решения задач профессиональной деятельности Уметь: выявлять и оценивать направления информационных угроз при решении задач профессиональной деятельности Владеть: навыками организации защиты информации при решении задач профессиональной деятельности
ОПК-3	Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ОПК-3.1	Осуществляет поиск, сбор, хранение, обработку, представление информации при решении задач профессиональной деятельности	Знать: правовые нормы и основные принципы сбора, обработки, хранения и передачи информации Уметь: работать с информационно справочными системами Владеть: навыками работы с автоматизированными информационно справочными системами и с телекоммуникационными сетями
		ОПК-3.2	Подбирает и использует информационные технологии при решении задач профессиональной деятельности	знать: стандартные задачи профессиональной деятельности на основе информационной и библиографической структуры с применением информационно-коммуникационных технологий уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий владеть: навыками решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

12. Объем дисциплины в зачетных единицах/час— 3/108.

Форма промежуточной аттестации: *зачет.*

13. Виды учебной работы

Вид учебной работы		Трудоемкость	
		Всего	По семестрам
			8 семестр
Аудиторные занятия		52	52
в том числе:	лекции	26	26
	практические	–	–
	лабораторные	26	26

Самостоятельная работа	56	56
в том числе: курсовая работа (проект)	-	-
Форма промежуточной аттестации *(зачет – __час.)*		зачет
Итого:	108	108

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1	Введение в теорию информационной безопасности	Основные понятия и определения. Концептуальные основы информационной безопасности и защиты информации	https://edu.vsu.ru/enrol/index.php?id=7597
2	Структура информационных ресурсов. Интеллектуальная собственность и коммерческая тайна.	Понятие об информационных ресурсах. Понятия интеллектуальной собственности и коммерческой тайны, их структура. Персональные данные. Принципы информационной безопасности.	https://edu.vsu.ru/enrol/index.php?id=7597
3	Угрозы информационной безопасности и их классификация.	Угрозы информационным ресурсам: угрозы несанкционированного доступа, модификации и удаления информации; угрозы криминогенного характера, природного и техногенного характера, угрозы, связанные с неквалифицированным пользованием информационными ресурсами. Компьютерный шпионаж, его цели и методы. Внутренние и внешние факторы, способствующие компьютерному шпионажу. Характеристика каналов утечки информации. Активный и пассивный доступ к информационным ресурсам.	https://edu.vsu.ru/enrol/index.php?id=7597
4	Правовые аспекты защиты информации.	Понятие о правовых средствах защиты информации. Законы, регулирующие деятельность по защите информации. Охрана объектов интеллектуальной собственности. Проблемы, возникающие при реализации правовых мер защиты информации.	https://edu.vsu.ru/enrol/index.php?id=7597
5	Организационные мероприятия, направленные на защиту информации.	Ограничение и разграничение доступа к информации. Дублирование важной информации на разнотипных носителях. Многоуровневая система защиты информации.	https://edu.vsu.ru/enrol/index.php?id=7597
6	Программно-аппаратные средства защиты информации	Пароли и системы с многоуровневым доступом. «Защита от дурака» в компьютерных программах. Защита программ и электронных баз данных. Антивирусные программы. Защита каналов связи. Повреждение информации в каналах связи и средства борьбы с ним.	https://edu.vsu.ru/enrol/index.php?id=7597
7	Математические методы и модели в задачах защиты информации.	Методы сжатия информации. Криптографические методы защиты информации. Шифрование с симметричными и ассимметричными ключами.	https://edu.vsu.ru/enrol/index.php?id=7597
8	Эффективность мероприятий по защите информации	Частный функциональный критерий информационной безопасности и его формула для мероприятий по предотвращению несанкционированного доступа. Структура понесенного и предотвращенного ущерба от несанкционированного доступа к информации. Структура затрат на защиту информации.	https://edu.vsu.ru/enrol/index.php?id=7597

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)			
		Лекции	Лабораторные	Самостоятельная работа	Всего
1	Введение в теорию информационной безопасности	2	2	2	6
2	Структура информационных ресурсов. Интеллектуальная собственность и коммерческая тайна.	2	2	8	12
3	Угрозы информационной безопасности и их классификация.	4	4	8	16
4	Правовые аспекты защиты информации.	4	4	6	14
5	Организационные мероприятия, направленные на защиту информации.	4	4	6	14
6	Программно-аппаратные средства защиты информации	2	2	8	12
7	Математические методы и модели в задачах защиты информации.	6	6	12	24
8	Эффективность мероприятий по защите информации	2	2	6	10
	Итого	26	26	56	108

14. Методические указания для обучающихся по освоению дисциплины

Преподавание дисциплины заключается в чтении лекций и проведении лабораторных занятий. На лекциях рассказывается теоретический материал, на лабораторных занятиях решаются примеры по теоретическому материалу, прочитанному на лекциях. При изучении курса «Информационная безопасность» обучающимся следует внимательно слушать и конспектировать материал, излагаемый на аудиторных занятиях. Для его понимания и качественного усвоения обучающимся рекомендуется следующая последовательность действий.

1. После каждой лекции студентам рекомендуется подробно разобрать прочитанный теоретический материал, выучить все определения, разобрать примеры, решенные на лекции. Перед следующей лекцией обязательно повторить материал предыдущей лекции.
2. Перед лабораторным занятием обязательно повторить лекционный материал. После лабораторного занятия еще раз разобрать решенные на этом занятии примеры, после приступить к выполнению домашнего задания. Если при решении примеров, заданных на дом, возникают вопросы, обязательно задать на следующем лабораторном занятии или в присутствующий час преподавателю.
3. При подготовке к лабораторным занятиям повторить основные понятия по темам, изучить примеры. Решая задачи, предварительно понять, какой теоретический материал нужно использовать. Наметить план решения, попробовать на его основе решить лабораторные задачи.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины *(список литературы оформляется в соответствии с требованиями ГОСТ и используется общая сквозная нумерация для всех видов источников)*

№ п/п	Источник
1	*Мельников, Владимир Павлович. Информационная безопасность и защита информации : учебное пособие для студ. вузов, обуч. по специальности 230201 "Информационные системы и технологии" / В.П. Мельников, С.А. Клейменов, А.М. Петраков ; под ред. С.А. Клейменова .— М. : ACADEMIA, 2006 .— 330 с. : ил .— (Высшее профессиональное образование. Информатика и вычислительная техника) .— Библиогр.: с.327-328 .— ISBN 5-7695-2592-4.*
2	*Чубукова, Светлана Георгиевна. Основы правовой информатики (юридические и математические вопросы информатики) : учебное пособие для студ. / С.Г. Чубукова, В.Д. Элькин*

	; Моск. гос. юрид. акад.; под ред. М.М. Рассолова .— М. : Контракт, 2004 .— 247 с. : ил. — На обл. авт. не указан .— Библиогр. в конце глав .— ISBN 5-900785-84-X.программирование / А.В. Аграновский, Р.А. Хади .— М. : СОЛОН-Пресс, 2002 .— 254, [1] с. : ил.
3	*Иванов, Михаил Александрович. Криптографические методы защиты информации в компьютерных системах и сетях / Иванов М. А. — М. : Кудиц-Образ, 2001 .— 363 с. : ил.*
4	*Астанин, Иван Константинович. Защита информации : учебное пособие для вузов / И.К. Астанин, Н.И. Астанин ; Воронеж. гос. ун-т, Лискинский филиал .— Воронеж : Воронеж. гос. ун-т, 2006 .— Библиогр. : с.169 .— ISBN 5-9273-1080-x.*

* Вначале указываются ЭБС, с которыми имеются договора у ВГУ, затем открытые электронно-образовательные ресурсы

16. Перечень учебно-методического обеспечения для самостоятельной работы

(учебно-методические рекомендации, пособия, задачники, методические указания по выполнению практических (контрольных) работ и др.)

№ п/п	Источник
5	*Скоромников, Кир Серафимович. Компьютерное право Российской Федерации : Учебник / К.С.Скоромников;Междунар.независим. эколого-политол.ун-т .— М. : Изд-во МНЭПУ, 2000 .— 220,[1] с. — ISBN 5-7383-0105-6.*
6	*Велпури, Рама. Oracle8i : Резервное копирование и восстановление / Р. Велпури, А. Адколи ; Пер.с англ. И. Афанасьева; Науч. ред. А. Головко; Авт. предислов. Я. Текер .— М. : Лори, 2002 .— 572 с. : ил .— Парал. тит. л. англ. — ISBN 5-85582-166-8.*
7	*Гайдамакин, Н.А. Разграничение доступа к информации в компьютерных системах / Н.А. Гайдамакин .— Екатеринбург : Изд-во Уральского ун-та, 2003 .— 327 с. : ил .— Библиогр.:с.317-322 .— Алф.-предм. указ.: с.306-316 .— ISBN 5-86037-024-5.*
8	*Голуб, Владимир Александрович. Информационная безопасность телекоммуникационных систем : Учебное пособие .— Воронеж : Студия ИАН, 2002 .— 157,[1] с. — ISBN 5-86026-020-2 : 37.00 .— <URL:http://www.lib.vsu.ru/elib/books/b102829.djvu>.*

17. Информационные технологии, используемые для реализации учебной дисциплины, включая программное обеспечение и информационно-справочные системы (при необходимости)

Дисциплина может реализовываться с применением электронного обучения и дистанционных образовательных технологий. При проведении занятий в дистанционной форме используются технические и информационные ресурсы Образовательного портала "Электронный университет ВГУ" (https://edu.vsu.ru), базирующегося на системе дистанционного обучения Moodle, развернутой в университете, а также другие доступные ресурсы в сети Интернет.

№ п/п	Источник
1	*www.fstec.ru, www.securitylab.ru , www.cyberpol.ru , www.azi.ru , www.infotecs.ru , www.infosec.ru , www.infoforum.ru , www.cnews.ru , www.brighttalk.com , www.coresecurity.com .*

18. Материально-техническое обеспечение дисциплины:

(при использовании лабораторного оборудования указывать полный перечень, при большом количестве оборудования можно вынести данный раздел в приложение к рабочей программе)

Компьютеры, с установленным программным обеспечением: Microsoft Visual Studio, LibreOffice.

Для проведения лекционных и лабораторных занятий используются аудитории, соответствующие действующим санитарно-техническим нормам и противопожарным правилам.

Для проведения лабораторных занятий и самостоятельной работы используется класс с компьютерной техникой, оснащенный необходимым программным обеспечением, электронными учебными пособиями и законодательно - правовой и нормативной поисковой системой, имеющий выход в глобальную сеть.

19. Оценочные средства для проведения текущей и промежуточной аттестаций

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:

№ п/п	Наименование раздела дисциплины	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
1	Введение в теорию информационной безопасности	ОПК-1, ОПК-3, ОПК-4	ОПК-1.1, ОПК-1.2, ОПК-1.3, ОПК-3.1, ОПК-3.2, ОПК-4.1, ОПК-4.2	Домашнее задание, контрольная работа
2	Структура информационных ресурсов. Интеллектуальная собственность и коммерческая тайна.	ОПК-1, ОПК-3, ОПК-4	ОПК-1.1, ОПК-1.2, ОПК-1.3, ОПК-3.1, ОПК-3.2, ОПК-4.1, ОПК-4.2	Домашнее задание, контрольная работа
3	Угрозы информационной безопасности и их классификация.	ОПК-1, ОПК-3, ОПК-4	ОПК-1.1, ОПК-1.2, ОПК-1.3, ОПК-3.1, ОПК-3.2, ОПК-4.1, ОПК-4.2	Домашнее задание, контрольная работа
4	Правовые аспекты защиты информации.	ОПК-1, ОПК-3, ОПК-4	ОПК-1.1, ОПК-1.2, ОПК-1.3, ОПК-3.1, ОПК-3.2, ОПК-4.1, ОПК-4.2	Домашнее задание, контрольная работа
5	Организационные мероприятия, направленные на защиту информации.	ОПК-1, ОПК-3, ОПК-4	ОПК-1.1, ОПК-1.2, ОПК-1.3, ОПК-3.1, ОПК-3.2, ОПК-4.1, ОПК-4.2	Домашнее задание, контрольная работа
6	Программно-аппаратные средства защиты информации	ОПК-1, ОПК-3, ОПК-4	ОПК-1.1, ОПК-1.2, ОПК-1.3, ОПК-3.1, ОПК-3.2, ОПК-4.1, ОПК-4.2	Домашнее задание, контрольная работа
7	Математические методы и модели в задачах защиты информации.	ОПК-1, ОПК-3, ОПК-4	ОПК-1.1, ОПК-1.2, ОПК-1.3, ОПК-3.1, ОПК-3.2, ОПК-4.1, ОПК-4.2	Домашнее задание, контрольная работа
8	Эффективность мероприятий по защите информации	ОПК-1, ОПК-3, ОПК-4	ОПК-1.1, ОПК-1.2, ОПК-1.3, ОПК-3.1, ОПК-3.2, ОПК-4.1, ОПК-4.2	Домашнее задание, контрольная работа
	Промежуточная аттестация форма контроля – зачёт и экзамен			Перечень вопросов Практическое задание

20 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1 Текущий контроль успеваемости

Текущая аттестация проводится в форме лабораторных работ и контрольной работы.

20.2 Промежуточная аттестация

Промежуточная аттестация по дисциплине осуществляется с помощью следующих оценочных средств:

Собеседование по билетам к зачету

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

Пример КИМ № 1

УТВЕРЖДАЮ
Заведующий кафедрой функционального
анализа и операторных уравнений

_____ Каменский М.И.
подпись, расшифровка подписи

__.__.__

Направление подготовки / специальность ___01.03.04 Прикладная математика_____

Дисциплина_____Б1.О.ДВ.36 Защита информации_____

Форма обучения _____очная_____
очное, очно-заочное, заочное

Вид контроля _____зачет_____
экзамен, зачет

Вид аттестации _____промежуточная_____
текущая, промежуточная

Контрольно-измерительный материал № ___

1. Угрозы информационной безопасности.

2. Методы и средства инженерной защиты объектов информатизации

Преподаватель _____ _____.
подпись расшифровка подписи

Пример контрольного задания (вариант задания)

Контрольная работа
по дисциплине «Защита информации»

Вариант №___

В результате шифрования методом Вижинера был получен следующий шифртекст: «СПЦСЗЗЮУГИВЕБЬБТЖЩИОБ». Прочитайте этот шифртекст, если известно, что шифрующая последовательность содержит только символы А, Б и В.

Оценка знаний, умений и навыков, характеризующая этапы формирования компетенций в рамках изучения дисциплины осуществляется в ходе текущей и промежуточной аттестаций.

Текущая аттестация проводится в форме лабораторных работ и контрольной работы.

Промежуточная аттестация проводится в форме зачета и включает в себя теоретические вопросы, позволяющие оценить уровень полученных знаний и практическое задание, позволяющее оценить степень сформированности умений и навыков.

При оценивании используется следующая шкала:

Зачтено ставится, если обучающийся демонстрирует полное или удовлетворительное соответствие знаний, умений, навыков приведенным в таблицах показателям, свободно или с незначительными ошибками оперирует приобретенными знаниями, умениями, применяет их при решении практических задач;

Не зачтено ставится, если обучающийся демонстрирует явное несоответствие знаний, умений, навыков приведенным в таблицах показателям.

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Обучающийся в полной мере владеет понятийным аппаратом в области программирования и технологии работы на ЭВМ, способен иллюстрировать ответ примерами, фактами, применять теоретические знания для решения практических задач программирования, СУБД и сетевых технологий.	*Повышенный уровень*	*Зачтено*
У обучающегося сформированы знания, умения и навыки программирования и технологии работы на ЭВМ; он способен иллюстрировать ответ примерами, фактами, применять теоретические знания для решения практических задач; но допускает отдельные несущественные пробелы в своих знаниях, допускает ошибки при выполнении практических задач.	*Базовый уровень*	
У обучающегося сформированы неполные знания, умения и навыки; он допускает отдельные существенные пробелы в своих знаниях, допускает существенные ошибки при выполнении практических задач.	*Пороговый уровень*	
Сформированы лишь фрагментарные знания, умения и навыки или знания, умения и навыки отсутствуют	*–*	*Не Зачтено*

20.3 Фонд оценочных средств сформированности компетенций студентов, рекомендуемый для проведения диагностических работ

1) (Вставить три слова) – это набор документированных норм, правил и практических приемов, регулирующих управление, защиту и распределение информации ограниченного доступа

Ответ: Политика информационной безопасности

2) К правовым методам, обеспечивающим информационную безопасность, относятся:

A. Разработка аппаратных средств обеспечения правовых данных;
B. Разработка и установка во всех компьютерных правовых сетях журналов учета действий;
C. Разработка и конкретизация правовых нормативных актов обеспечения безопасности.

Ответ: C)**Разработка и конкретизация правовых нормативных актов обеспечения безопасности**

1) Присвоение субъектам и объектам идентификаторов с целью получения доступа к информации и сопровождаемая ее проверка подлинности субъекта по предъявленному им идентификатору для принятия решения о предоставлении ему доступа к ресурсам системы – это _____.

Ответ: **Идентификация и аутентификация**

2) Свойство, которое гарантирует, что защищаемая информация не может быть доступна или раскрыта для неавторизованных личностей, объектов или процессов – это _____

Ответ: **Конфиденциальность**

3) Согласно принципу Керхгоффса, надёжность криптографической системы определяться:

A. Секретностью аппаратно-программного функционирования криптосистемы;
B. Секретностью используемых алгоритмов шифрования или их особенностей;
C. Только секретностью используемого ключа или ключей шифрования;
D. Секретностью используемых алгоритмов и ключей шифрования.

Ответ: D **Секретностью используемых алгоритмов и ключей шифрования**

4) Утечкой информации в системе называется ситуация, характеризуемая:

A. Потерей защищаемой информации в системе;
B. Неконтролируемое распространение защищаемой информации;
C. Изменением формы или содержания защищаемой информации.

Ответ: B **Неконтролируемое распространение защищаемой информации**

1) Метод управления доступом, при котором каждому идентифицированному объекту и субъекту системы присваивается метка секретности, определяющая ценность информации называется_____.

Ответ: **Мандатным**

2) Присоединяемое к сообщению его криптографическое преобразование, которое позволяет при получении сообщения другим пользователем проверить нго авторство и подлинность называется_____.

Ответ: **Электронной подписью**

3) Раздел прикладной математики, изучающий модели, методы, алгоритмы, программные и аппаратные средства анализа криптосистемы или ее входных и выходных сигналов с целью извлечения конфиденциальных параметров, включая открытый текст называется _____.

Ответ: **Криптоанализ**

4) Установить взаимно однозначное соответствие между угрозами защищаемой информации:

1) потеря ценности информации при ее раскрытии;
2) потеря ценности информации при ее модификации или уничтожении;
3) потеря ценности информации при невозможности ее оперативного использования;
4) потеря ценности информации при сбоях в информационных системах;

и нарушениями свойств защищаемой информации

а) нарушение целостности;
б) нарушение конфиденциальности;
в) нарушение устойчивости к ошибкам;
г) нарушение доступности.

Ответ: **1б, 2а, 3г, 4в.**

5) Символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов, этот метод называется:

A. гаммированием;
B. подстановкой;
C. кодированием;
D. перестановкой;
E. аналитическим преобразованием.

Ответ: B **Подстановкой**

Задания раздела 20.3 рекомендуются к использованию при проведении диагностических работ с целью оценки остаточных результатов освоения данной дисциплины (знаний, умений, навыков).