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

УТВЕРЖДАЮ

Заведующий кафедрой
функционального анализа и операторных уравнений
наименование кафедры, отвечающей за реализацию дисциплины
Каменский М.И.
подпись, расшифровка подписи
26.06.2018 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.В.ДВ.4.2 Математические основы криптологии

1. Код и наименование направления подготовки/специальности: 01.03.04 Прикладная математика

2. Профиль подготовки/специализация:

3. Квалификация (степень) 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 №0500-07 от 03.07.2018

8. Учебный год: 2018-2019 **Семестр(ы):** 8

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

Цель курса - изучение основных принципов, методов и средств защиты информации в процессе ее обработки, передачи и хранения с использованием компьютерных средств в информационных системах.

Основными задачами изучения дисциплины являются:

- изучение характеристик основных угроз информационной безопасности, каналов утечки информации и методов компьютерного шпионажа;
- получение представлений о существующих правовых, организационных методах и технических средствах защиты информации от несанкционированного доступа и от модификации и удаления;
- освоение критериев эффективности мер по защите информации.

10. Место учебной дисциплины в структуре ООП:

Дисциплина входит в вариативную часть (дисциплины по выбору) математического и естественнонаучного цикла. Для изучения и освоения дисциплины нужны знания из предшествующих курсов: Теория графов и математическая логика, Теория вероятностей, математическая статистика и теория случайных процессов, Алгоритмы дискретной математики, Операционные системы и сети, Программные аппаратные средства информатики, Программирование для ЭВМ. 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):

Компетенция		Планируемые результаты обучения
Код	Название	
ОПК-1	готовность к самостоятельной работе	знать: общие проблемы безопасности, роль и место информационной безопасности на современном этапе развития общества; правовые основы защиты информации; основные методы криптографической защиты информации; методы защиты информации в вычислительных сетях; технические средства обеспечения безопасности; принципы функционирования компьютерных вирусов и методы борьбы с ними; уметь: использовать полученные знания для организации безопасной работы персональных компьютеров и сетуй на их основе; использовать программно-аппаратные средства защиты от несанкционированного доступа и модификации информации; защищать ресурсы персональных компьютеров и сетуй на их основе от компьютерных вирусов и их вредного воздействия; владеть**:** навыками работы со специальной литературой; навыками работы со специализированным программно-аппаратным обеспечением компьютерной безопасности.
ОПК-2	способность использовать современные математические методы и современные прикладные	знать: современные математические методы и современные прикладные программные средства уметь: использовать современные математические методы

	программные средства и осваивать современные технологии программирования	и современные прикладные программные средства и осваивать современные технологии программирования владеть: навыками работы с современными прикладными программными средствами и с специализированным программно-аппаратным обеспечением компьютерной безопасности
ПК-9	способность выявить естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности, готовностью использовать для их решения соответствующий естественнонаучный аппарат	знать: как выявить естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности, готовностью использовать для их решения соответствующий естественнонаучный аппарат уметь: использовать для решения проблем, возникающих в ходе профессиональной деятельности соответствующий естественнонаучный аппарат. владеть: способностью выявить естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности, готовностью использовать для их решения соответствующий естественнонаучный аппарат
ПК-11	готовность применять знания и навыки управления информацией	знать: особенности управления информацией уметь: применять знания и навыки управления информацией владеть: навыками поиска информации по особенностям конкретной поставленной задачи
ПК-10	готовность применять математический аппарат для решения поставленных задач, способностью применить соответствующую процессу математическую модель и проверить ее адекватность, провести анализ результатов моделирования, принять решение на основе полученных результатов	Знать: как применять математический аппарат для решения поставленных задач и для разработки программ. Уметь: применять математический аппарат для решения поставленных задач. Владеть: способностью применить соответствующую процессу математическую модель и проверить ее адекватность, провести анализ результатов моделирования, принять решение на основе полученных результатов

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

Форма промежуточной аттестации: зачет.

13. Виды учебной работы

Вид учебной работы	Трудоемкость (часы)	
	Всего	По семестрам
		сем. № 8
Аудиторные занятия	*28*	*28*
в том числе: лекции	*24*	*24*
практические	-	-
лабораторные	*24*	*24*

Самостоятельная работа	*60*	*60*
Форма промежуточной аттестации	*зачет*	*зачет*
Итого:	*108*	*108*

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
1	Предмет криптологии и этапы ее развития	Основные задачи криптологии. Криптография и криптоанализ. Основные понятия и определения. Этапы развития криптологии. Роль математики в развитии методов защиты информации.
2	Арифметические и статистические основы простейших криптосистем	Математическая модель открытого текста. Простейшие методы шифрования с закрытым ключом. Математические модели простейших шифров.
3	Математические методы криптоанализа простейших симметричных систем	Индекс совпадения и взаимный индекс совпадения. Тест Казиски. Дешифрование шифров моно- и полиалфавитной замены. Дешифрование шифров перестановки.
4	Математические модели симметричных криптосистем. Стандартные криптосистемы с симметричным ключом	Шеноновские модели криптосистем. Основные типы шифров. Методы шифрования с закрытым ключом. Блочный и потоковый шифры. Группа шифрующих преобразований, их свойства и взаимосвязь со стойкостью. Математические модели криптосистем DES, IDEA, ГОСТ 28147-89.
5	Математические методы криптоанализа симметричных систем	Методы криптоанализа на основе теории статистических решений. Разностный и линейный криптоанализ. Теоретико-информационные оценки стойкости симметричных криптосистем
6	Арифметические и алгебраические основы криптосистем с ассимметричным ключом	Проблемы простоты числа и факторизации числа. Критерии простоты числа. Проблемы дискретного логарифмирования.
7	Математические модели ассимметричных криптосистем. Математические методы криптоанализа ассимметричных систем	Рюкзачный метод шифрования и его стойкость. L^3 -атака на рюкзачный метод шифрования. Криптосистема RSA и ее стойкость. Атаки на криптосистему RSA при неудачном выборе ее параметров (на основе теоремы Ферма, повторным шифрованием, на основе Китайской теоремы об остатках, безключевым чтением). Криптосистемы Эль-Гамаля, Рабина, и их стойкость.
8	Новые направления в криптологии	Мультибазисная криптография. Возможности квантовой криптографии. Математическое разделение секрета. Активный криптоанализ.

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)			
		Лекции	Лабораторные	Самостоятельная работа	Всего
1	Предмет криптологии и этапы ее развития	3	3	8	14
2	Арифметические и статистические основы простейших криптосистем	3	3	8	14
3	Математические методы криптоанализа простейших симметричных систем	3	3	8	14

4	Математические модели симметричных криптосистем. Стандартные криптосистемы с симметричным ключом	3	3	6	12
5	Математические методы криптоанализа симметричных систем	3	3	6	12
6	Арифметические и алгебраические основы криптосистем с ассимметричным ключом	3	3	8	14
7	Математические модели ассимметричных криптосистем. Математические методы криптоанализа ассимметричных систем	3	3	8	14
8	Новые направления в криптологии	3	3	8	14
					0
	Итого	24	24	60	108

14. Методические указания для обучающихся по освоению дисциплины

Аудиторные занятия, лекции и лабораторные занятия, предполагают самостоятельную работу студентов по данному курсу. Ряд тем выносятся для самостоятельного изучения, предлагаются темы для создания докладов с презентациями. Предусмотрены домашние задания и оформление отчетов выполнения лабораторных заданий, а также дополнительные задания для сильных студентов.

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	*Аграновский, Александр Владимирович. Практическая криптография : Алгоритмы и их программирование / А.В. Аграновский, Р.А. Хади .— М. : СОЛОН-Пресс, 2002 .— 254, [1] с. : ил.*
2	*Иванов, Михаил Александрович. Криптографические методы защиты информации в компьютерных системах и сетях / Иванов М. А. — М. : Кудиц-Образ, 2001 .— 363 с. : ил.*
3	*Майорова С.П. Алгебра : учебное пособие / С.П. Майорова, М.Г. Завгородний. – Воронеж : ГОУВПО «Воронеж. гос. техн. ун-т», 2007. – Ч. 2 – 130 с.*
4	*Майорова С.П. Алгебра : учебное пособие / С.П. Майорова, М.Г. Завгородний. – Воронеж : ГОУВПО «Воронеж. гос. техн. ун-т», 2008. – Ч. 3 – 102 с.*

* 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	*Коробейников А.Г. Математические основы криптологии : учебное пособие / А.Г. Коробейников, Ю.А. Гатчин. – СПб : СПб ГУ ИТМО, 2004. – 106 с.*
6	*Галуев Г.А. Математические основы криптологии : учебно-методическое пособие / Г.А. Галуев. –*

	Таганрог : Изд-во ТРТУ, 2003. – 120с.
7	*Жданов О. Н. Криптоанализ классических шифров : лабораторный практикум / Жданов О. Н., Куденкова И. А. – Красноярск, 2008. – 107 с.*

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

№ 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)

Лекционная аудитория (доска, мел, маркеры), Компьютерный класс (14-15 компьютеров + программное обеспечение) мультимедийный проектор.

19. Фонд оценочных средств:

19.1 Перечень компетенций с указанием этапов формирования и планируемых результатов обучения

Код и содержание компетенции (или ее части)	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенции посредством формирования знаний, умений, навыков)	Этапы формирования компетенции (разделы (темы) дисциплины или модуля и их наименование)	ФОС* (средства оценивания)
ОПК-1 готовность к самостоятельной работе	знать: общие проблемы безопасности, роль и место информационной безопасности на современном этапе развития общества; правовые основы защиты информации; основные методы криптографической защиты информации; методы защиты информации в вычислительных сетях; технические средства обеспечения безопасности; принципы функционирования компьютерных вирусов и методы борьбы с ними;	1-8	Устный опрос. Лабораторные занятия.Тесты для самопроверки по темам.
	уметь: использовать полученные знания для организации безопасной	1-8	

	работы персональных компьютеров и сетуй на их основе; использовать программно-аппаратные средства защиты от несанкционированного доступа и модификации информации; защищать ресурсы персональных компьютеров и сетуй на их основе от компьютерных вирусов и их вредного воздействия;		
	владеть: навыками работы со специальной литературой; навыками работы со специализированным программно-аппаратным обеспечением компьютерной безопасности.	1-8	
ОПК-2 способность использовать современные математические методы и современные прикладные программные средства и осваивать современные технологии программирования	знать: современные математические методы и современные прикладные программные средства	1-8	Устный опрос. Лабораторные занятия.Тесты для самопроверки по темам.
	уметь: использовать современные математические методы и современные прикладные программные средства и осваивать современные технологии программирования	1-8	
	владеть: навыками работы с современными прикладными программными средствами и с специализированным программно-аппаратным обеспечением компьютерной безопасности	1-8	
ПК-9 способность выявить естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности, готовностью использовать для их решения соответствующий естественнонаучный аппарат	знать: как выявить естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности, готовностью использовать для их решения соответствующий естественнонаучный аппарат	1-8	Устный опрос. Лабораторные занятия.Тесты для самопроверки по темам.
	уметь: использовать для решения проблем, возникающих в ходе профессиональной деятельности соответствующий естественнонаучный аппарат.	1-8	
	владеть: способностью	1-8	

	выявить естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности, готовностью использовать для их решения соответствующий естественнонаучный аппарат		
ПК-11 готовность применять знания и навыки управления информацией	знать: особенности управления информацией	1-8	Устный опрос. Лабораторные занятия.Тесты для самопроверки по темам.
	уметь: применять знания и навыки управления информацией	1-8	
	владеть: навыками поиска информации по особенностям конкретной поставленной задачи	1-8	
ПК-10 готовность применять математический аппарат для решения поставленных задач, способностью применить соответствующую процессу математическую модель и проверить ее адекватность, провести анализ результатов моделирования, принять решение на основе полученных результатов	Знать: как применять математический аппарат для решения поставленных задач и для разработки программ.	1-8	Устный опрос. Лабораторные занятия.Тесты для самопроверки по темам.
	Уметь: применять математический аппарат для решения поставленных задач	1-8	
	Владеть: способностью применить соответствующую процессу математическую модель и проверить ее адекватность, провести анализ результатов моделирования, принять решение на основе полученных результатов	1-8	
Промежуточная аттестация			КИМ

19.2 Описание критериев и шкалы оценивания компетенций (результатов обучения) при промежуточной аттестации

Оценка знаний, умений и навыков, характеризующая этапы формирования компетенций в рамках изучения дисциплины осуществляется в ходе текущей и промежуточной аттестаций.
Для оценивания результатов обучения на зачете используется – зачтено, не зачтено
Соотношение показателей, критериев и шкалы оценивания результатов обучения.

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*	
Ответ на контрольно-измерительный материал не соответствует четырем из перечисленных показателей. Обучающийся демонстрирует отрывочные, фрагментарные знания, допускает грубые ошибки.	–	*Незачтено*

19.3 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.В.ДВ.4.2 Математические основы криптологии_____

Форма обучения _____очная_____
очное, очно-заочное, заочное

Вид контроля _____зачет_____
экзамен, зачет

Вид аттестации _____промежуточная_____
текущая, промежуточная

Контрольно-измерительный материал № ___

1. Математическая модель открытого текста.

2. Атаки на RSA. Циклическая атака.

Преподаватель _____ _____.
подпись расшифровка подписи

Пример контрольного задания (вариант задания)

Контрольная работа

по дисциплине «Математические основы криптологии»

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.

19.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Текущий контроль представляет собой проверку усвоения учебного материала теоретического и практического характера, регулярно осуществляемую на занятиях. К основным формам текущего контроля можно отнести устный опрос, проверку домашних заданий, лабораторные работы, контрольные работы. Промежуточная аттестация предназначена для определения уровня освоения всего объема учебной дисциплины «Математические основы криптологии» в форме зачета. Промежуточная аттестация, как правило, осуществляется в конце семестра и может завершать изучение как отдельной дисциплины, так и ее разделов. Промежуточная аттестация помогает оценить более крупные совокупности знаний и умений, в некоторых случаях даже формирование определенных профессиональных компетенций. На зачете оценивается практический уровень освоения дисциплины и степень сформированности компетенций оценками «зачтено», «не зачтено». Задания текущего контроля и проведение промежуточной аттестации должны быть направлены на оценивание уровня освоения теоретических и практических понятий, научных основ профессиональной деятельности; степени готовности обучающегося применять теоретические и практические знания и практически значимую информацию; приобретение умений профессионально значимых для профессиональной деятельности.