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

УТВЕРЖДАЮ
Заведующий кафедрой
математического анализа

А.Д. Баев
(подпись)
03.07.2018

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Б1.В.ДВ.08.02 Криптология

1. Код и наименование направления подготовки/специальности:

02.03.01 Математика и компьютерные науки

2. Профиль подготовки/специализация: Математические методы в экономике и финансах

3. Квалификация (степень) выпускника: Бакалавр

4. Форма обучения: Очная

5. Кафедра, отвечающая за реализацию дисциплины: Кафедра математического анализа

6. Составители программы:
Шабров Сергей Александрович, канд. Физ.-мат. наук, доцент

7. Рекомендована: Научно-методическим советом математического факультета, протокол №0500-07 от 03.07.2018г.

_____
(наименование рекомендующей структуры, дата, номер протокола,

_____
отметки о продлении вносятся вручную)

_____

8. Учебный год:2018-2019 **Семестр(ы):7**

9. Цели и задачи учебной дисциплины:

Целью дисциплины является подготовка специалиста, владеющего основополагающими методами и средствами защиты информационных систем с помощью криптографических методов.Цели изучения дисциплины:

Задачами дисциплины являются:

- изучение российского законодательства и стандартов в области криптографической защиты информации;
- изучение основных методов шифрования;
- изучение криптографических протоколов с примерами их использования при решении практических задач;
- изучение базовых алгоритмов, применяемых в криптосистемах;
- освоение основ криптоанализа;
- ознакомление со стеганографическими методами защиты информации;
- ознакомление с основами кодирования информации.

10. Место учебной дисциплины в структуре ООП:

Дисциплина относится к математическому и естественнонаучному циклу ФГОС ВПО в структуре ООП бакавриата. Для изучения дисциплины слушатели должны владеть базовыми знаниями школьного курса «Информатика» в области алгоритмизации и программирования.

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-2		Знать: криптографические протоколы. протоколы обмена ключами, протоколы электронной цифровой подписи. Уметь: использовать криптографические протоколы. протоколы обмена ключами, протоколы электронной цифровой подписи. Владеть: навыками использования криптографические протоколы. протоколы обмена ключами, протоколы электронной цифровой подписи.
ОПК-3		Знать: криптографические протоколы. протоколы обмена ключами, протоколы электронной цифровой подписи. Уметь: использовать криптографические протоколы. протоколы обмена ключами, протоколы электронной цифровой подписи. Владеть: навыками использования криптографические протоколы. протоколы обмена ключами, протоколы электронной цифровой подписи.
ОПК-4		Знать: криптографические протоколы. протоколы обмена ключами, протоколы электронной цифровой подписи. Уметь: использовать криптографические протоколы. протоколы обмена ключами, протоколы электронной цифровой подписи. Владеть: навыками использования криптографические

		протоколы. протоколы обмена ключами, протоколы электронной цифровой подписи.

12. Объем дисциплины в зачетных единицах/час.(*в соответствии с учебным планом)* **— 1** /32.

Форма промежуточной аттестации*(зачет/экзамен) зачет* .

13. Виды учебной работы

Вид учебной работы	Трудоемкость			
	Всего	По семестрам		
		№ семестра	№ семестра	7
Аудиторные занятия	32			32
в том числе: лекции	16			16
практические				
лабораторные	16			16
Самостоятельная работа				
Форма промежуточной аттестации *(зачет – 0 час. / экзамен – __час.)*				
Итого:	32			32

13.1. Содержание дисциплины

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
1. Лекции		
1.1	Основы информационной безопасности и защита информации. История криптографии.	Информация и информационная безопасность, основные составляющие информационной безопасности, объекты защиты, категории и носители информации, средства защиты информации. Наивная криптография, формальная криптография, математическая криптография.
1.2	Основные термины и определения. Классификация шифров.	Основные термины и определения, основные требования к криптосистемам, классификация криптографических систем. Шифры замены. Основы шифрования, шифры: однозначной замены, полиалфавитные, омофонические, полиалфавитные. Шифры перестановки. Основы шифрования, шифры одинарной и множественной перестановки. Шифры гаммирования. Основы шифрования, шифрование по модулю N и 2, генерация гаммы, генераторы гамм. Комбинированные шифры. Основы шифрования, ADFGX, DES, ГОСТ 28147-89. Шифрование с открытым ключом. Основы шифрования, алгоритм RSA, алгоритм на основе задачи об укладке ранца, вероятностное шифрование, алгоритм шифрования Эль-Гамаля, алгоритм на основе эллиптических кривых. Хеш-функции. Основные понятия, MD5, применение шифрования для получения хеш-образа
1.3	Криптографические протоколы. протоколы обмена ключами.	Основные сведения о криптографических протоколах, протоколы обмена ключами. Протоколы аутентификации (идентификации). Общие сведения, парольная идентификация / аутентификация, протокол идентификации / аутентификации с использованием хеш-функции, протокол идентификации / аутентификации на основе шифрования с открытым ключом, сервер

		аутентификации Kerberos, идентификация / аутентификация с помощью биометрических данных, идентификационные карты (ID-cards) и электронные ключи.
1.4	Протоколы электронной цифровой подписи.	Общие сведения, протокол на базе алгоритма RSA, алгоритм цифровой подписи ГОСТ 34.10-94, алгоритм цифровой подписи ГОСТ 34.10-2001, разновидности ЭЦП. Протоколы контроля целостности. Общие сведения, использование контрольных сумм, использование ЭЦП, использование MAC-кодов, проверка четности, использование ECC, комбинированные методы. Протоколы электронных платежей. Общие сведения, пластиковые карты, суррогатные платежные средства в Internet, расчеты пластиковыми карточками в Internet, электронные кошелки в Internet, цифровые деньги. Протоколы голосования. Общие сведения, некоторые варианты реализации протоколов электронного голосования, российский опыт электронного голосования. Другие протоколы. Протокол разделения секрета, протокол подбрасывания монеты "по телефону", тайные многосторонние вычисления. Некоторые сведения из теорий алгоритмов и чисел. Сложность алгоритмов, простые числа, разложение числа на простые сомножители, нахождение начального списка простых чисел, тестирование числа на простоту, определение наибольшего общего делителя.
1.5	Основы криптоанализа.	Угрозы безопасности при использовании криптографии, общие сведения о криптоанализе, разновидности атак на криптосистемы. Стеганография. Общие сведения, классическая стеганография, компьютерная стеганография. Кодирование информации. Общие сведения, общедоступные и секретные кодовые системы, номенклаторы.
3. Лабораторные работы		
3.1	Основы информационной безопасности и защита информации. История криптографии.	Информация и информационная безопасность, основные составляющие информационной безопасности, объекты защиты, категории и носители информации, средства защиты информации. Наивная криптография, формальная криптография, математическая криптография.
3.2	Основные термины и определения. Классификация шифров.	Основные термины и определения, основные требования к криптосистемам, классификация криптографических систем. Шифры замены. Основы шифрования, шифры: однозначной замены, полиалфавитные, омофонические, полиалфавитные. Шифры перестановки. Основы шифрования, шифры одинарной и множественной перестановки. Шифры гаммирования. Основы шифрования, шифрование по модулю N и 2, генерация гаммы, генераторы гамм. Комбинированные шифры. Основы шифрования, ADFGX, DES, ГОСТ 28147-89. Шифрование с открытым ключом. Основы шифрования, алгоритм RSA, алгоритм на основе задачи об укладке ранца, вероятностное шифрование, алгоритм шифрования Эль-Гамаля, алгоритм на основе эллиптических кривых. Хеш-функции. Основные понятия, MD5, применение шифрования для получения хеш-образа
3.3	Криптографические протоколы. протоколы обмена ключами.	Основные сведения о криптографических протоколах, протоколы обмена ключами. Протоколы аутентификации (идентификации). Общие сведения, парольная идентификация / аутентификация, протокол идентификации / аутентификации с использованием хеш-функции, протокол идентификации / аутентификации на основе

		шифрования с открытым ключом, сервер аутентификации Kerberos, идентификация / аутентификация с помощью биометрических данных, идентификационные карты (ID-cards) и электронные ключи.
3.4	Протоколы электронной цифровой подписи.	Общие сведения, протокол на базе алгоритма RSA, алгоритм цифровой подписи ГОСТ 34.10-94, алгоритм цифровой подписи ГОСТ 34.10-2001, разновидности ЭЦП. Протоколы контроля целостности. Общие сведения, использование контрольных сумм, использование ЭЦП, использование MAC-кодов, проверка четности, использование ECC, комбинированные методы. Протоколы электронных платежей. Общие сведения, пластиковые карты, суррогатные платежные средства в Internet, расчеты пластиковыми карточками в Internet, электронные кошелки в Internet, цифровые деньги. Протоколы голосования. Общие сведения, некоторые варианты реализации протоколов электронного голосования, российский опыт электронного голосования. Другие протоколы. Протокол разделения секрета, протокол подбрасывания монеты "по телефону", тайные многосторонние вычисления. Некоторые сведения из теорий алгоритмов и чисел. Сложность алгоритмов, простые числа, разложение числа на простые сомножители, нахождение начального списка простых чисел, тестирование числа на простоту, определение наибольшего общего делителя.
3.5	Основы криптоанализа.	Угрозы безопасности при использовании криптографии, общие сведения о криптоанализе, разновидности атак на криптосистемы. Стеганография. Общие сведения, классическая стеганография, компьютерная стеганография. Кодирование информации. Общие сведения, общедоступные и секретные кодовые системы, номенклаторы.

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела) дисциплины	Виды занятий (часов)				
		Лекции	Практические	Лабораторные	Самостоятельная работа	Всего
01	Основы информационной безопасности и защита информации. История криптографии.	2		2		4
02	Основные термины и определения. Классификация шифров.	4		4		8
03	Криптографические протоколы. протоколы обмена ключами.	2		2		4
04	Протоколы электронной цифровой подписи.	4		4		8
05	Основы криптоанализа.	4		4		8
	Итого	16		16		32

14. Методические указания для обучающихся по освоению дисциплины

работа с конспектами лекций

(рекомендации обучающимся по освоению дисциплины: работа с конспектами лекций, презентационным материалом, выполнение практических заданий, тестов, заданий текущей аттестации и т.д.)

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)*

а) основная литература:

№ п/п	Источник
1	Голуб, Владимир Александрович. Информационная безопасность СМИ: криптографическая защита информации : учебное пособие / В.А. Голуб ; Воронеж. гос. ун-т, Фак. журналистики .— Воронеж : Факультет журналистики ВГУ, 2010 .— 99 с.

б) дополнительная литература:

№ п/п	Источник
2	Мещеряков Р. В. Информационная безопасность: Учеб. пособие – Томск.: Изд-во Том. политехн. Ун-т, 2004 – 168 с.
3	Мещеряков Р. В., Шелупанов А. А. Специальные вопросы информационной безопасности. – Томск.: Изд-во ИОА ТНЦ СО РАН, 2003 – 250 с.
4	Мещеряков Р. В., Шелупанов А. А., Белов Е. Б., Лось В. П. Основы информационной безопасности. – М.: Горячая линия – Телеком, 2006. – 540 с.
5	Герасименко В. А. Защита информации в автоматизированных системах обработки данных. В 2-х кн. – М.: Энергоатомиздат, 1994.
6	Герасименко В. А., Малюк А. А. Основы защиты информации. – М.: «Инкомбук», 1997. – 540 с.

в)информационные электронно-образовательные ресурсы (официальные ресурсы интернет)*:

№ п/п	Ресурс
1.	*Электронный каталог Научной библиотеки Воронежского государственного университета. – (http // www.lib.vsu.ru/)*
2.	*Google, Yandex, Rambler*

* 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
1	Мещеряков Р. В. Информационная безопасность: Учеб. пособие – Томск.: Изд-во Том. политехн. Ун-т, 2004 – 168 с.
2	Мещеряков Р. В., Шелупанов А. А. Специальные вопросы информационной безопасности. – Томск.: Изд-во ИОА ТНЦ СО РАН, 2003 – 250 с.

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

---

18. Материально-техническое обеспечение дисциплины: компьютерный класс

---

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 - 2	Знать: криптографические протоколы. протоколы обмена ключами, протоколы электронной цифровой подписи.	Все разделы	Опрос
	Уметь: использовать криптографические протоколы. протоколы обмена ключами, протоколы электронной цифровой подписи.	Все разделы	Опрос
	Владеть: навыками использования криптографические протоколы. протоколы обмена ключами, протоколы электронной цифровой подписи.	Все разделы	Опрос
ОПК -3	Знать: криптографические протоколы. протоколы обмена ключами, протоколы электронной цифровой подписи.	Все разделы	Опрос
	Уметь: использовать криптографические протоколы. протоколы обмена ключами, протоколы электронной цифровой подписи.	Все разделы	Опрос
	Владеть: навыками использования криптографические протоколы. протоколы обмена ключами, протоколы электронной цифровой подписи.	Все разделы	Опрос
ОПК -4	Знать: криптографические протоколы. протоколы обмена ключами, протоколы электронной цифровой подписи.	Все разделы	Опрос
	Уметь: использовать криптографические протоколы. протоколы обмена ключами, протоколы электронной цифровой подписи.	Все разделы	Опрос
	Владеть: навыками использования криптографические протоколы. протоколы обмена ключами, протоколы электронной цифровой подписи.	Все разделы	Опрос
Промежуточная аттестация			КИМ

* В графе «ФОС» в обязательном порядке перечисляются оценочные средства текущей и промежуточной аттестаций.

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

1) знание учебного материала и владение понятийным аппаратом;
2) умение связывать теорию с практикой;
3) умение иллюстрировать ответ примерами, фактами, данными научных исследований;
4) умение применять полученные знания на практике;
5) владение понятийным аппаратом данной области науки (теоретическими основами дисциплины), способность иллюстрировать ответ примерами, фактами, данными научных исследований, применять теоретические знания для решения практических задач.

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Обучающийся в полной мере владеет понятийным аппаратом данной области науки (теоретическими основами дисциплины), способен иллюстрировать ответ примерами, фактами, данными научных исследований, применять теоретические знания для решения практических задач в области…	*Повышенный уровень*	*зачет*
Обучающийся владеет понятийным аппаратом данной области науки (теоретическими основами дисциплины), допускает не значительные ошибки при ответе.	*Базовый уровень*	*зачет*
Обучающийся владеет частично теоретическими основами дисциплины, фрагментарно способен дать ответ .	*Пороговый уровень*	*зачет*
Обучающийся демонстрирует отрывочные, фрагментарные знания, допускает грубые ошибки,	–	*Незачет*

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

19.3.1 Перечень вопросов к экзамену (зачету): (нужное выбрать)

1. Понятия "информационная безопасность" и "защита информации". Основные составляющие информационной безопасности.
2. Объекты защиты. Категории и носители информации.
3. Средства защиты информации.
4. Криптография. Основные термины и определения.
5. Классификация криптографических систем.
6. Шифры замены. Основные методы шифрования.
7. Шифры перестановки. Основные методы шифрования.
8. Шифры гаммирования. Основные методы шифрования.
9. Шифры гаммирования. Способы генерации гаммы. Генераторы гамм.
10. Схема режима шифрования DES-ECB.
11. Схема режима шифрования DES-CBC.
12. Схема режима шифрования DES-CPB и DES-OFB.
13. Тройной DES. Сферы применения различных режимов DES.
14. Схема режима шифрования простой замены ГОСТ 28147-89.
15. Шифрование с открытым ключом. Основные понятия.
16. Алгоритм шифрования RSA.
17. Алгоритм шифрования Эль-Гамаля.
18. Алгоритм шифрования на основе задачи об укладке ранца.
19. Эллиптические кривые. Основные понятия. Сложение и умножение точки.
20. Алгоритм шифрования на основе эллиптических кривых.
21. Хэш-функции. Основные понятия и разновидности.
22. Хэш-функция. MD5.
23. Криптографические протоколы. Основные понятия.

24. Протоколы обмена ключами.
25. Протоколы аутентификации. Разновидности и краткая характеристика.
26. Парольная идентификация/аутентификация.
27. Протокол идентификации/аутентификации на основе шифрования с открытым ключом.
28. Сервер аутентификации Kerberos.
29. Идентификация/аутентификация с помощью биометрических данных.
30. Идентификационные карты (ID-cards) и электронные ключи.
31. Электронная цифровая подпись. Общие сведения и разновидности ЭЦП.
32. ЭЦП на базе алгоритма RSA.
33. Алгоритм цифровой подписи ГОСТ 34.10-94.
34. Алгоритм цифровой подписи ГОСТ 34.10-2001.
35. Протоколы контроля целостности.
36. Электронные платежи.
37. Классическое ("бумажное") голосования.
38. Российский опыт электронного голосования.
39. Протокол разделения секрета.
40. Протокол подбрасывания монеты по телефону.
41. Тайные многосторонние вычисления.
42. Сложность алгоритмов.
43. Простые числа.
44. Разложение числа на простые сомножители.
45. Нахождение начального списка простых чисел.
46. Тестирование числа на простоту.
47. Определение наибольшего общего делителя.
48. Основные сведения о криптоанализе и атаки на криптосистемы.
49. Классическая стеганография.
50. Компьютерная стеганография.
51. Общие сведения о кодировании.
52. Общедоступные кодовые системы.
53. Секретные кодовые системы.

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.

Промежуточная аттестация предназначена для определения уровня освоения всего объема учебной дисциплины 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 компетенций.

На зачете оценивается практический уровень освоения дисциплины и степень сформированности компетенций оценками «зачет» и «не зачет».

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.