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

УТВЕРЖДАЮ

Заведующий кафедрой программного обеспечения
и администрирования информационных систем

Артемов М. А.

08.06.2018 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Б1.В.11 Криптология

1. Код и наименование направления подготовки:

02.03.03 Математическое обеспечение и администрирование информационных систем

2. Профиль подготовки: Информационные системы и базы данных

3. Квалификация (степень) выпускника: бакалавр

4. Форма обучения: очная

5. Кафедра, отвечающая за реализацию дисциплины:

программного обеспечения и администрирования информационных систем

6. Составители программы:

Барановский Е.С., кандидат физико-математических наук

7. Рекомендована: НМС факультета ПММ протокол № 10 от 18.06.2018 г.

8. Учебный год: 2018/2019 **Семестр:** 6

9. Цели и задачи учебной дисциплины: ознакомление студентов с современным положением дел в области хранения, обработки, поиска, передачи, преобразования, закрытия и восстановления конфиденциальной информации в организациях и предприятиях, а также формирование навыков защиты от несанкционированного доступа к ней.

10. Место учебной дисциплины в структуре ООП: Дисциплина относится к вариативной части Блока 1. Дисциплина имеет логические и

содержательнометодические связи с дисциплиной Б1.Б.31 Информационная безопасность.

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	способность применять в профессиональной деятельности знания математических основ информатики	Знать: область применения, терминологию, основные задачи и методы криптографии и криптоанализа. Уметь: применять криптографические методы преобразования, передачи, закрытия и восстановления конфиденциальной информации, а также использовать методы управления ключами. Владеть: навыками программирования алгоритмов криптографической защиты информации.

12. Объем дисциплины в зачетных единицах/часах в соответствии с учебным планом — 4 ЗЕТ/ 144 часа. **13. Виды учебной работы**

Вид учебной работы	Трудоемкость (часы)	
	Всего	Сем. 6
Аудиторные занятия	64	64
в том числе: лекции	32	32
лабораторные	32	32
практические	-	-
Самостоятельная работа	44	44
Итого	108	108
Форма промежуточной аттестации	36	36
Итого:	**144**	**144**

13.1. Содержание разделов дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
1	Введение в криптологию.	Общие и исторические сведения криптологии. Основные понятия и классические шифры.
2	Математические основы криптологии.	Множества и отображения. Множества с алгебраическими операциями. Бинарные операции. Группы, кольца, поля. Сравнения. Кольцо классов вычетов.

3	Симметрические криптосистемы.	Подстановки. Системы шифрования Вижинера. Перестановки. Гаммирование. Блочные шифры.
4	Криптосистемы с открытым ключом.	Односторонние функции. Генерация ключей. Алгоритм Диффи-Хеллмана. Криптосистема RSA. Криптосистема Эль-Гамаля.
5	Аутентификация и электронная подпись.	Протоколы аутентификации. Цифровая подпись. Формирование и алгоритмы проверки подписи.
6	Правовые основы деятельности по защите информации.	Основные определения в области информационного права. Вопросы правового регулирования отношений в области защиты информации.

13.2. Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)				
		Лекции	Лабораторные	Практические	Самостоятельная работа	Всего
1	Введение в криптологию.	2	4	-	4	10
2	Математические основы криптологии.	6	6	-	16	28
3	Симметрические криптосистемы.	8	8	-	10	26
4	Криптосистемы с открытым ключом.	8	8	-	6	22
5	Аутентификация и электронная подпись.	6	6	-	6	18
6	Правовые основы деятельности по защите информации.	2	-	-	2	4
	Итого:	32	32	-	44	108

14. Методические указания для обучающихся по освоению дисциплины

Работа с конспектами лекций, чтение литературы.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины

а) основная литература:

№ п/п	Источник
1	Основы управления информационной безопасностью: [учебное пособие для студентов вузов, обучающихся по направлениям подготовки (специальностям) укрупненной группы специальностей 090000 - "Информ. безопасность"] / А.П. Курило [и др.] .— 2-е изд., испр. — Москва: Горячая Линия-Телеком, 2014 .— 243 с.
2	Информатика: базовый курс: [учебное пособие для студ. втузов]; под ред. С.В. Симоновича.— 3-е изд. — СПб. [и др.] : Питер, 2012 .— 637 с.
3	Глухов М. М., Круглов И. А., Пичкур А. Б., Черемушкин А. В. Введение в теоретикочисловые методы криптографии. —СПб.: Лань, 2011. — 400 с. http://e.lanbook.com/books/element.php?pl1_id=1540

б) дополнительная литература:

№ п/п	Источник

4	Коробейников А. Г., Гатчин Ю. А. Математические основы криптологии [Электронный ресурс] : — Электрон. дан. — СПб.: Издательство НИУ ИТМО, 2004. — 106 с. — http://e.lanbook.com/books/element.php?pl1_id=43393
5	Ян Сонг Й. Криптоанализ RSA. — Москва-Ижевск: Регулярная и хаотическая динамика: Ижевский институт компьютерных исследований, 2011 .— 285 с.
6	Пролубников А.В. Криптографические средства защиты информации в сетях: учебнометодическое пособие [Электронный ресурс]: — Электрон. дан.— Омск: Издательство Омского государственного университета им. Ф.М. Достоевского, 2014 г. — 192 с. — http://www.knigafund.ru/books/174111

в) информационные электронно-образовательные ресурсы**:**

№ п/п	Источник
7	Электронный каталог Научной библиотеки Воронежского государственного университета. – http://www.lib.vsu.ru/
8	ЭБС «Издательство Лань» http://e.lanbook.com/

18. Материально-техническое обеспечение дисциплины: Аудитория с проектором и доской.

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	ФОС* (средства оценивания)
ОПК-2 способность применять в профессиональной деятельности знания математических основ информатики	Знать: область применения, терминологию, основные задачи и методы криптографии и криптоанализа.	Раздел 1, раздел 6.	Опрос
	Уметь: применять криптографические методы преобразования, передачи, закрытия и восстановления конфиденциальной информации, а также использовать методы управления ключами.	Разделы 2–5.	Опрос
	Владеть: навыками программирования алгоритмов криптографической защиты информации.	Разделы 2–5.	Опрос
Промежуточная аттестация			Комплект КИМ

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

Для оценивания результатов обучения на экзамене/зачете используются следующие показатели:

1) знание теоретического материала:

2) хорошее понимание материала, умение рассуждать; 3) умение приводить собственные примеры;
4) умение решать задачи.

Для оценивания результатов обучения на экзамене) используется 4-балльная шала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Соотношение показателей, критериев и шкалы оценивания результатов обучения.

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Отличное знание теоретического материала, умение рассуждать, приводить примеры и решать задачи повышенной сложности.	*Повышенный уровень*	*Отлично*
Хорошее знание теоретического материала и владение понятийным аппаратом. Умение проиллюстрировать материал примерами. Способность решать стандартные задачи.	*Базовый уровень*	*Хорошо*
Удовлетворительное знание теоретического материала. Способность к решению несложных задач. Допустимы незначительные недочеты в ответах.	*Пороговый уровень*	*Удовлетворительно*
Существенные пробелы в изучении курса.	–	*Неудовлетворительно*

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:

1. Предмет криптологии. Криптография и криптоанализ: основные задачи, методы, этапы развития.
2. Классические шифры. Подстановка и перестановка. Таблица Виженера.
3. Гаммирование.
4. Блочные шифры и их применение.
5. Множества с алгебраическими операциями.
6. Делимость целых чисел. Наибольший общий делитель. Алгоритм Евклида.
7. Линейное представление наибольшего общего делителя.
8. Взаимно простые числа и их основные свойства.
9. Простые числа и их основные свойства. Простейший алгоритм проверки числа на «на простоту».
10. Основная теорема арифметики. Каноническое представление числа.
11. Расположение простых чисел в числовом ряду. Асимптотический закон распределения простых чисел.
12. Сравнения и их основные свойства.
13. Понятие группы. Порядок группы. Подгруппа.
14. Понятие кольца и поля. Идеал. Главный идеал. Класс вычетов по идеалу.

15. Кольцо вычетов по данному модулю. Полные системы вычетов и их свойства.
16. Структура кольца вычетов Z_m. Приведенная система вычетов. Мультипликативная группа обратимых элементов в Z_m.
17. Примитивные элементы поля Z_p и их применение при построении криптоситем.
18. Функция Эйлера и способ ее вычисления.
19. Теорема Эйлера, малая теорема Ферма и ее следствие.
20. Решения сравнений. Равносильные сравнения. Способы упрощения сравнений.
21. Решение сравнений первой степени. Явные формулы для нахождения решений.
22. Диофантовы уравнения и способы их решения.
23. Односторонние функции. Функции с секретом.
24. Алгоритм Диффи-Хеллмана генерации ключей.
25. Атака «Человек посередине» на криптосистему Диффи-Хеллмана.
26. Криптосистема RSA.
27. Криптосистема Эль-Гамаля.
28. Генерация ключей ассиметричных криптосистем.
29. Протоколы аутентификации. Цифровая подпись.
30. Алгоритмы проверки подписи.
31. Правовое регулирование отношений в области защиты информации.

19.3.2 Перечень практических заданий

Примеры практических заданий:

1. Известно, что абонент A, используя схему шифрования Эль-Гамаля, каждый раз применяет один и тот же сессионный ключ при зашифровывании своих сообщений. Первый шифротекст (a1, b1) = (1389, 15144), переданный абоненту B, удалось расшифровать – это сообщение Q1 = 14908. Известна первая компонента открытого ключа: p = 37097. Определите второе сообщение Q2, зашифрованное через (a2, b2) = (1389, 23683), не используя процедуру нахождения секретного ключа.
2. Алиса и Боб решили сгенерировать секретный ключ на основе алгоритма Диффи-Хеллмана. Для этого они выбрали открытый ключ: m=101, q=59. Затем Алиса выбрала свой секретный ключ α=79, а Боб – свой секретный ключ β=43. Определите общий секретный ключ k Алисы и Боба.
3. Постройте множество примитивных элементов поля Z_p при заданном простом числе p.
4. Алиса сформировала открытый ключ (p, g, y) = (99961, 92201, 87678) на основе схемы Эль-Гамаля (для электронной подписи) и передала его абоненту Бобу. Выбрав сессионный ключ k = 83507 и секретный ключ x = 23898, Алиса отправила Бобу сообщение Q = 40097 с соответствующей электронной подписью. Определите, какую подпись сообщения Q получил Боб.

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

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

Текущая аттестация проводится в соответствии с Положением о текущей аттестации обучающихся по программам высшего образования Воронежского государственного университета. Текущая аттестация проводится в форме опроса.

Промежуточная аттестация проводится в соответствии с Положением о промежуточной аттестации обучающихся по программам высшего образования.

Контрольно-измерительные материалы промежуточной аттестации включают в себя теоретический вопрос. Предполагаются дополнительные вопросы и задачи.

При оценивании используются количественные шкалы оценок. Критерии оценивания приведены выше.