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.
02.04.2024г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.В.ДВ.04.01 Теоретические основы обработки информации

1. Код и наименование направления подготовки/специальности:

09.03.03 Прикладная информатика

2. Профиль подготовки/специализация:

Прикладная информатика в юриспруденции

3. Квалификация (степень) выпускника:

Бакалавриат

4. Форма обучения:

Очная

5. Кафедра, отвечающая за реализацию дисциплины:

Кафедра программного обеспечения и администрирования информационных систем

6. Составители программы:

доц. Барановский Е.С., к. ф.-м. н., доц.

7. Рекомендована:

НМС факультета ПММ, протокол № 5 от 22.03.2024

8. Учебный год:

2024-2025

9. Цели и задачи учебной дисциплины:

Цель изучения дисциплины: изучение основ теории информации и ознакомление студентов с математическими и компьютерными аспектами криптологии.

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:

Учебная дисциплина относится к Блоку Б1.

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

Код и название компетенции	**Код и название индикатора компетенции**	**Знания, умения, навыки**
ОПК-1 Способен применять естественнонаучные и общеинженерные знания, методы математического анализа и моделирования, теоретического и экспериментального исследования в профессиональной деятельности;	ОПК-1.1 Решает типовые задачи с учетом основных понятий и общих закономерностей, сформулированных в рамках базовых дисциплин математики, информатики и естественных наук.	Знать: Математические основы теории информации и криптологии
		Уметь: использовать симметрические криптосистемы
	ОПК-1.2 Применяет системный подход и математические методы для формализации решения прикладных задач. ОПК-1.3 Осуществляет выбор современных математических инструментальных средств для обработки исследуемых явлений в соответствии с поставленной задачей, анализирует результаты расчетов и интерпретирует полученные результаты.	Владеть: основными методами криптологического анализа
ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;	ОПК-3.1 Применяет типовые математические модели на практике ОПК-3.2 Модифицирует выбранную математическую модель при разработке программных продуктов	Знать: Математические основы теории информации и криптологии
		Уметь: использовать симметрические криптосистемы
		Владеть: основными методами криптологического анализа

12. Объем дисциплины в зачетных единицах/час:

3/108

Форма промежуточной аттестации:

Экзамен

13. Виды учебной работы

Вид учебной работы	Семестр 6	Всего
Аудиторные занятия	48	48
Лекционные занятия	32	32
Практические занятия		0
Лабораторные занятия	16	16
Самостоятельная работа	24	24
Промежуточная аттестация	36	36
Часы на контроль	36	36
Всего	108	108

13.1. Содержание дисциплины

п/п	Наименование раздела дисциплины	Содержание разделадисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1	Введение в теорию информации	Базовые понятия теории информации. Количественная оценка информации. Сжатие информации. Кодирование информации. Защита информации.	https://edu.vsu.ru/enrol/index.php?id=6171
2	Математические основы теории информации и криптологии.	Множества и отображения. Множества с алгебраическими операциями. Бинарные операции. Группы, кольца, поля. Сравнения. Кольцоклассов вычетов.	https://edu.vsu.ru/enrol/index.php?id=6171
3	Симметрические криптосистемы.	Подстановки. Системы шифрования Вижинера. Перестановки. Гаммирование. Блочные шифры.	https://edu.vsu.ru/enrol/index.php?id=6171

п/п	Наименование раздела дисциплины	Содержание разделадисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
4	Криптосистемы с открытым ключом.	Односторонние функции. Генерация ключей. Алгоритм Диффи-Хеллмана. Криптосистема RSA.	https://edu.vsu.ru/enrol/index.php?id=6171
5	Аутентификация и электронная подпись.	Протоколы аутентификации. Цифровая подпись. Формирование и алгоритмы проверки подписи.	https://edu.vsu.ru/enrol/index.php?id=6171

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела)	Лекционные занятия	Практические занятия	Лабораторные занятия	Самостоятельная работа	Всего
1	Введение в теорию информации	6		4	6	16
2	Математические основы теории информации и криптологии.	6		4	6	16
3	Симметрические криптосистемы.	6		4	4	14
4	Криптосистемы с открытым ключом.	6		2	4	12
5	Аутентификации электронная подпись.	8		2	4	14
		32	0	16	24	72

14. Методические указания для обучающихся по освоению дисциплины

Работа с конспектами лекций, чтение литературы.

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

№ 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

б) дополнительная литература:

№ п/п	Источник
1	Коробейников А. Г., Гатчин Ю. А. Математические основы криптологии [Электронный ресурс] : — Электрон. дан. — СПб.: Издательство НИУ ИТМО, 2004. — 106 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=43393

в) информационные электронно-образовательные ресурсы:

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

16. Перечень учебно-методического обеспечения для самостоятельной работы

№ п/п	Источник
1	Евдокимов, М. А. Основы криптологии : учебное пособие / М. А. Евдокимов, Е. А. Райков. — Самара : АСИ СамГТУ, 2016. — 78 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/127723 (дата обращения: 04.02.2021). — Режим доступа: для авториз. пользователей.

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

ОС Windows

18. Материально-техническое обеспечение дисциплины:

Аудитория с проектором, доска, лаборатория с компьютерами

19. Оценочные средства для проведения текущей и промежуточной аттестаций

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

№ п/п	Разделы дисциплины (модули)	Код компетенции	Код индикатора	Оценочные средства для текущей аттестации
1	1-5	ОПК-1	ОПК-1.1 ОПК-1.2 ОПК-1.3	КИМ
2	1-5	ОПК-3	ОПК-3.1 ОПК-3.2	КИМ

Промежуточная аттестация

Форма контроля - Экзамен

Оценочные средства для промежуточной аттестации

Критерии оценивания компетенций	**Уровень сформированности компетенций**	**Шкала оценок**
Отличное знание теоретического материала, правильное и эффективное решение задачи, правильный ответ на тест. Должны быть выполнены ВСЕ лабораторные работы.	Повышенный уровень	Отлично
Хорошее знание теоретического материала, в целом правильное решение задачи. НО: допускает незначительные ошибки в решении задачи. Неправильный ответ на тест. ИЛИ: выполнены все показатели повышенного уровня, но не зачтена одна лабораторная работа, но студент продемонстрировал умение решать задачи по этой теме (это задача в КИМе)	Базовый уровень	Хорошо
Решение задачи не доведено до конца или недостаточное знание теоретического материала. Неоптимальное решение задачи и недостаточное владение теоретическим материалом. Неправильный тест. ИЛИ: выполнены все показатели базового уровня, но не зачтено более одной лабораторной работы.	Пороговый уровень	Удовлетворительно
Задача не решена или серьезные пробелы в знании теоретического материала (с незнанием могут быть связаны и грубые ошибки в ответе на тестовые вопросы).	–	*Неудовлетворительно*

20 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1 Текущий контроль успеваемости

контрольная работа

20.2 Промежуточная аттестация

Примеры вопросов к экзамену:

1. Каноническое представление натурального числа.
2. Примеры атак на алгоритм Диффи–Хеллмана.
3. Криптосистема Эль-Гамаля.
4. Сформулируйте основные задачи криптографии.
5. Алгоритм Диффи–Хеллмана.
6. Электронная подпись на основе схемы Эль-Гамаля.
7. Мультипликативная группа обратимых элементов в Zm.
8. Два эквивалентных определения функции Эйлера.
9. Процедура аутентификации в рамках протокола Шнорра.
10. Процедура гаммирования.
11. Законы дистрибутивности для операций в кольце.
12. Криптосистема RSA.

Пример заданий для контрольной работы

Вариант 1

1. Известны следующие параметры, используемые в алгоритме Диффи–Хеллмана:
$m = 54311$, $q = 50131$, $x = 34101$, $y = 12904$.
Определите секретный ключ k.

2. Известна гамма γ = (2, 5, 14, 21, 3) и шифротекст ВРКДЛПНХБ. Определите исходное слово.

3. Известны следующие параметры, используемые в протоколе Шнорра:
$p = 33107$, $q = 16553$, $g = 2902$, $y = 9107$, $r = 32607$.
Абонент **B** направляет абоненту **A** число $e = 11997$. Какое подтверждение s после этого должен выслать абонент **A**?