Рабочая программа дисциплины

1. Название дисциплины: Теория кодирования и ее применения в криптографии

2. Уровень высшего образования – магистратура

3. Направление подготовки: 01.04.01 Математика (магистратура)

4. Аннотация:

Курс «Теория кодирования и ее применения в криптографии» является профильной дисциплиной магистерской программы «Математические методы защиты информации».

5. Объем дисциплины в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся (указывается согласно рабочему плану):

Объем дисциплины составляет 2 зачетные единицы, всего 72 часа, из которых 34 часа составляет контактная работа обучающегося с преподавателем (34 часов занятия лекционного типа), 38 часа составляет самостоятельная работа обучающегося.

6. Формируемые компетенции и входные требования для освоения дисциплины, предварительные условия:

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВПО по данному направлению:

a) **общекультурных (ОК):** владеть основными методами, способами и средствами получения, хранения, переработки информации, иметь навыки работы с компьютером как средством управления информацией (ОК-12);
b) **профессиональных (ПК):** детальное знание основ программирования, особенностей языков программирования общего и специального назначения, наиболее широко используемых средств программирования (ПК-18).

В результате освоения дисциплины студент должен:

знать - основные понятия, определения и факты теории кодирования(ОК-10);

уметь применять на практике основные методы теории кодирования (ОК-10);

понимать и применять на практике компьютерные технологии для решения различных задач криптографического анализа;

уметь находить, анализировать и обрабатывать научно-техническую информацию (ОК-10);

- извлекать полезную научно-техническую информацию из электронных библиотек, реферативных журналов (ПК-17);

- демонстрировать способность к анализу и синтезу (ОК-14);
- демонстрировать способность к письменному и устному общению на русском языке (ОК-15);
- публично представить собственные и известные научные результаты (ПК-18);
- представить математические знания в устной форме (ПК-27);

владеть навыками решения практических задач теории кодирования;

- методами использования теории кодирования при решении задач криптоанализа, проблемно-задачной формой представления математических знаний (ПК-22);
- проблемно-задачной формой представления естественнонаучных знаний (ПК-23).

Для освоения дисциплины необходимы знания и умения, приобретаемые в рамках курса «Алгебра», «Дискретная математика»,

7. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и виды учебных занятий

№ п/п	Раздел Дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)			Формы текущего контроля успеваемости *(по неделям семестра)* Форма промежуточной аттестации *(по семестрам)*
				Лекц	Прак	сам	

1	1. Передача информации по каналу связи. Помехи, ошибки. Расстояние Хэмминга. Кодовое расстояние. Обнаружение и корректирование ошибок. Линейный код. Порождающая матрица. Кодирование и декодирование с помощью порождающей матрицы. 2. Двойственный код. Проверочная матрица. Синдром. Кодовое расстояние линейного кода. Связь кодового расстояния со свойствами столбцов проверочной матрицы. Вектор ошибок. Исправление небольшого числа ошибок. Линейные коды с кодовыми расстояниями 1 и 2.	4	1	2	-	4	
2	3 Линейные коды с кодовым расстоянием 3. Двоичный код Хэмминга. Кодирование, исправление ошибок и декодирование с помощью двоичного кода Хэмминга. 4. Проблема верхних оценок мощности кодов. Рекуррентные оценки. 5. Оценка Хэмминга (граница сферической упаковки). Достижимость оценки Хэмминга	4	2	2	-	4	

	на коде Хэмминга. Совершенные коды.						
3	6. Оценка Синглтона для линейных и нелинейных кодов. 7. Оценка Джонсона. Следствие из нее. Связь между максимальными мощностями кода на всем множестве наборов и на его подмножестве. Оценка Элайеса–Бассалыго. 8. Оценка Плоткина и следствия из нее. Достижимость оценки Плоткина на коде, двойственном к коду Хэмминга.	4	3	2	-	4	
4	9. Матрицы Адамара. Делимость порядка матрицы Адамара на 4. Связь матриц Адамара и кодов с большими кодовыми расстояниями. Достижимость оценки Плоткина на кодах, построенных с помощью матрицы Адамара. Эквивалентность матриц Адамара и кодов, на которых достигается равенство в следствии из оценки Плоткина. Точное значение максимальной мощности двоичного кода в случае больших кодовых расстояний при условии	4	4	2	-	4	

	существования матриц Адамара						
5	10. Кронекерово произведение матриц. Кронекерово произведение матриц Адамара есть матрица Адамара. Матрица Адамара–Сильвестра. Квадратичные вычеты. Символы Лежандра. Построение матриц Адамара с помощью символов Лежандра. Построение матриц Адамара всех порядков до 100, делящихся на 4, кроме 92. 11. Оценка Грайсмера, ее достижимость на коде, двойственном к двоичному коду Хэмминга.	4	5	2	-	4	
6	12. Оценка Варшамова–Гильберта. 13. Двоичная энтропия. Выражение биномиальных коэффициентов через энтропию. Скорость кода. Асимптотические оценки скорости кода, получаемые через оценки Хэмминга, Элайеса–Бассалыго и Варшамова–Гильберта, их сравнение между собой. 14. Расширенный двоичный код Голея, его кодовое расстояние. Двоичный код Голея как совершенный код.	4	6	2	-	4	

7	15. Распределение весов кода. Теорема Шапиро–Злотника. 16. Тождества Мак-Вильямс. 17. Булевы функции. Полином Жегалкина. Код Рида–Маллера, его кодовое расстояние. Дуальный код к коду Рида–Маллера. Связь кода Рида–Маллера первого порядка с матрицей Адамара–Сильвестра.	4	7	4	-	8	
8	18. Мажоритарное декодирование кодов Рида–Маллера. 19. Радиус покрытия кода. Радиус покрытия кода Рида–Маллера первого порядка. Его значение для криптографии. 20. Быстрое умножение матрицы Адамара–Сильвестра на столбец.	4	8	4	-	8	
9	21. Матрица Вандермонда, ее невырожденность. Коды Рида–Соломона трех типов, их параметры. Достижимость оценки Синглтона на кодах Рида–Соломона. Коды, двойственные к кодам Рида–Соломона второго и третьего типа. 22. Циклические коды. Представление наборов линейных циклических кодов в виде многочленов. Линейный циклический код как идеал в	4	9	4	-	8	

	кольце классов вычетов многочленов. Порождающий многочлен. Проверочный многочлен. 23. Многочлен ошибок. Синдромный многочлен. Кодирование, исправление ошибок и декодирование линейных циклических кодов на языке многочленов.						
10	24. Код Рида–Соломона первого типа как циклический код. Порождающий многочлен кода Рида–Соломона первого типа. 25. Подполе и расширение поля. Коды Боуза–Чоудхури–Хоквингема (БЧХ), их проверочная матрица, оценки кодового расстояния и размерности. Коды Хэмминга и Рида–Соломона первого типа как частные случаи кода БЧХ. 26. Взаимосвязь множества наборов кода БЧХ над Fq с множеством наборов соответствующего кода Рида–Соломона над Fqm. Код БЧХ как циклический код. Примеры кодов БЧХ. Минимальные многочлены и сопряженные корни.	4	10-11	4	-	8	

	Порождающий многочлен кода БЧХ.						
11	27. Алгоритм декодирования Питерсона–Горенстейна–Цирлера для кодов БЧХ, его трудоемкость. 28. Проблема быстрого решения системы линейных уравнений специального вида при исправлении ошибок в коде БЧХ. Сведение к задаче нахождения регистра сдвига с линейной обратной связью минимальной длины, генерирующего данную последовательность. 29. Леммы о длине минимального регистра сдвига. 30. Алгоритм Берлекэмпа–Месси, его трудоемкость.	4	12-13	4	-	8	
12	31. Синдромный многочлен и многочлен значений ошибок для кода БЧХ. Алгоритм Форни нахождения значений ошибок. 32. Открытые системы шифрования на основе кодов, корректирующих ошибки. Системы открытого шифрования Мак-Элиса и Нидеррайтера. Сравнение систем открытого шифрования Мак-Элиса и	4	14	4	-	8	

	Нидеррайтера.						
13	33. Ортогональные массивы. Их параметры. Корреляционно-иммунные функции. Связь силы ортогонального массива, построенного по линейному коду, с кодовым расстоянием дуального кода. Существование ортогональных массивов из выполнения условия границы Варшамова– Гильберта. 34. Ортогональный массив, построенный с помощью кода Рида–Соломона. Конструкция Буша	4	15	4	-	8	
14	35. Коды аутентификации. Их построение с помощью ортогональных массивов. 36. Дизъюнктные коды. Построение системы разделения ключей с помощью дизъюнктных кодов. 37. Разделяющие коды. Каскадная конструкция дизъюнктных кодов.	4	16	4	-	8	

Лабораторные работы

Лабораторные работы не предусмотрены учебным планом

*Текущий контроль успеваемости в рамках занятий семинарского типа реализуется в форме по рейтинговой системе с учётом результатов проверки домашних заданий, работы в аудитории и результатов выполнения практических компьютерных заданий.

8. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

8.1. Самостоятельные работы.

Самостоятельные работы не предусмотрены учебным планом.

8.2 Примеры теоретических вопросов.

1. Оценка Синглтона для линейных и нелинейных кодов
2. Оценка Плоткина и следствия из нее.
3. Оценка Грайсмера, ее достижимость на коде, двойственном к двоичному коду Хэмминга.
4. Оценка Варшамова–Гильберта.
5. Быстрое умножение матрицы Адамара–Сильвестра на столбец.
6. Коды БЧХ
7. Алгоритм декодирования Питерсона–Горенстейна–Цирлера для кодов БЧХ
8. Коды аутентификации
9. Дизъюнктные коды
10. Разделяющие коды

9. Перечень основной и дополнительной учебной литературы

Основная литература

1. Сидельников Владимир Михайлович . Теория кодирования. М. Физматлит.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости):

При реализации учебной работы в рамках дисциплины «Теория кодирования и ее применения в криптографии» используются средства дистанционного сопровождения учебного процесса в форме сайтов с материалами лекций и семинарских занятий. Курс имеет электронные версии (презентации) лекций. Лекции читаются с использованием современных мультимедийных возможностей и проекционного оборудования.

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Любая аудитория, оснащенная проекционным оборудованием с возможностью подключения к ноутбуку, экраном, и учебной доской.