**Санкт-Петербургский государственный университет**

**Р А Б О Ч А Я П Р О Г Р А М М А**

**УЧЕБНОЙ ДИСЦИПЛИНЫ**

Криптография

Cryptography

**Язык(и) обучения**

русский

Трудоемкость в зачетных единицах: 2

Регистрационный номер рабочей программы: 001931

**Раздел 1. Характеристики учебных занятий**

**1.1. Цели и задачи учебных занятий**

Ввести обучающихся в теорию помехоустойчивого кодирования, ознакомить с классическими двоичными кодами. Провести анализ свойств булевых функций и двоичных полиномов с точки зрения их приложений в области кодирования. Для закрепления лекционного материала и расширения тематики разобрать на занятиях ряд прикладных алгоритмов и обсудить отдельные доклады, самостоятельно подготовленные слушателями на основе научных публикаций.

**1.2. Требования подготовленности обучающегося к освоению содержания учебных занятий (пререквизиты)**

Знание основ информатики и математики.

**1.3. Перечень результатов обучения (learning outcomes)**

Знания о задачах корректирующего кодирования и подходах к их решению, о конкретных схемах кодирования и декодирования, о математических основах алгоритмов.

Умение: анализировать математические модели задач кодирования в рамках материала курса, осуществлять кодирование и декодирование с использованием изученных алгоритмов, рассчитывать числовые характеристики кодов.

Приобретение и закрепление навыков целенаправленного поиска информации в различных источниках, включая сетевые ресурсы сети Интернет, для решения профессиональных задач.

**1.4. Перечень и объём активных и интерактивных форм учебных занятий**

В качестве основных интерактивных форм предполагается, что самостоятельную работу в предлагаемом курсе обучающиеся выполняют с использованием компьютера.

**Раздел 2. Организация, структура и содержание учебных занятий**

**2.1. Организация учебных занятий**

**2.1.1 Основной курс**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Трудоёмкость, объёмы учебной работы и наполняемость групп обучающихся | | | | | | | | | | | | | | | | | | |
| Код модуля в составе дисциплины,  практики и т.п. | Контактная работа обучающихся с преподавателем | | | | | | | | | | | | Самостоятельная работа | | | | Объём активных и интерактивных  форм учебных занятий | Трудоёмкость |
| лекции | семинары | консультации | практические  занятия | лабораторные работы | контрольные работы | коллоквиумы | текущий контроль | промежуточная  аттестация | итоговая аттестация | под руководством преподавателя | в присутствии  преподавателя | сам. раб. с использованием  методических материалов | текущий контроль (сам.раб.) | промежуточная аттестация (сам.раб.) | итоговая аттестация  (сам.раб.) |
| ТРАЕКТОРИЯ 7 СЕМЕСТРА | | | | | | | | | | | | | | | | | | |
| Форма обучения: очная | | | | | | | | | | | | | | | | | | |
| Семестр 7 | 30 |  | 2 |  |  |  |  |  | 2 |  |  | 30 |  |  | 8 |  | 30 | 2 |
|  | 2-100 |  | 2-100 |  |  |  |  |  | 2-100 |  |  | 10-25 |  |  | 1-1 |  |  |  |
| ИТОГО | 30 |  | 2 |  |  |  |  |  | 2 |  |  | 30 |  |  | 8 |  |  | 2 |
| ТРАЕКТОРИЯ 8 СЕМЕСТРА | | | | | | | | | | | | | | | | | | |
| Форма обучения: очная | | | | | | | | | | | | | | | | | | |
| Семестр 8 | 24 |  | 2 |  |  |  |  |  | 2 |  |  | 24 |  |  | 20 |  | 2 | 2 |
|  | 2-100 |  | 2-100 |  |  |  |  |  | 2-100 |  |  | 10-25 |  |  | 1-1 |  |  |  |
| ИТОГО | 24 |  | 2 |  |  |  |  |  | 2 |  |  | 24 |  |  | 20 |  |  | 2 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Виды, формы и сроки текущего контроля успеваемости и промежуточной аттестации | | | | | | |
| Код модуля в составе дисциплины, практики и т.п. | Формы текущего контроля успеваемости | | Виды промежуточной аттестации | | Виды итоговой аттестации  (только для программ итоговой аттестации и дополнительных образовательных программ) | |
| Формы | Сроки | Виды | Сроки | Виды | Сроки |
| ТРАЕКТОРИЯ 7 СЕМЕСТРА | | | | | | |
| Форма обучения: очная | | | | | | |
| Семестр 7 |  |  | экзамен, устно, традиционная форма | по графику промежуточной аттестации |  |  |
| ТРАЕКТОРИЯ 8 СЕМЕСТРА | | | | | | |
| Форма обучения: очная | | | | | | |
| Семестр 8 |  |  | экзамен, устно, традиционная форма | по графику промежуточной аттестации |  |  |

**2.2. Структура и содержание учебных занятий**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  | | --- | --- | --- | --- | | **№ п.п.** | **Наименование темы (раздела, части)** | **Вид учебных занятий** | **Кол-во часов** | | 1 | Тема 1. Двоичные корректирующие коды. | лекции | 18 | | сам. раб. в присутствии  преподавателя | 18 | | 2 | Тема 2. Линейные коды над GF(2). | лекции | 126 | | сам. раб. в присутствии  преподавателя | 12 | | 3 | Промежуточная аттестация | консультации | 2 | | самостоятельная работа | 8 | | экзамен | 2 | | 4 | Тема 3. Коды Рида-Маллера. | лекции | 24 | | сам. раб. в присутствии  преподавателя | 24 | | 5 | Промежуточная аттестация | консультации | 2 | | самостоятельная работа | 20 | | экзамен | 2 | | **Итого** | | | **144** |   **Тема 1. Двоичные корректирующие коды.**  Коды, исправляющие ошибки. Блочные коды. Кодовое расстояние. Границы избыточности. Код Хэмминга. Коды Адамара.  **Тема 2. Линейные коды над GF(2).**  Проверочная и порождающая матрицы. Двойственные коды. Смежные классы. Совершенные коды. Код Голея.  **Тема 3.** Коды Рида-Маллера.  Определение и свойства кодов Рида–Маллера. Коды 1-го и 2-го порядка. Алгоритмы кодирования и декодирования. |

**Раздел 3. Обеспечение учебных занятий**

**3.1. Методическое обеспечение**

**3.1.1 Методические указания по освоению дисциплины**

Успешное освоение дисциплины возможно благодаря посещению лекций, участию в обсуждении вопросов, подготовленных к занятию, выполнению индивидуальных заданий, самостоятельной работе, включающей в себя чтение специальной литературы по разделам темы, подготовку докладов по тематике курса.

**3.1.2 Методическое обеспечение самостоятельной работы**

Самостоятельная работа обучающихся в рамках данной дисциплины является важным компонентом обучения, предусмотренным компетентностно-ориентированным учебным планом и рабочей программой учебной дисциплины.

Настоящей программой предусмотрены формы самостоятельной работы в писутствии преподавателя.

Одна из форм самостоятельной работы – это подготовка докладов по тематике курса с использованием источников, перечисленных в списке обязательной и дополнительной литературы в данной программе.

**3.1.3 Методика проведения текущего контроля успеваемости и промежуточной аттестации и критерии оценивания**

В течение семестра по отдельным темам требуется выполнение письменных заданий во время занятий либо дома. Тем, кто не выполнил часть заданий, аналогичные задачи предлагаются во время экзамена.

Методика проведения экзамена

Экзамен проводятся в устной форме. Билет состоит из одного теоретического вопроса и двух задач. Время подготовки ответа на вопросы билета составляет не более 40 минут. После ответа на вопрос билета и проверки решения задач преподаватель задает несколько дополнительных вопросов, ответы на которые также влияют на итоговую оценку.

Критерии выставления оценок:

1. Оценка «отлично»: выполнены в установленный срок все индивидуальные задания по курсу; правильные ответы на вопросы билета и дополнительные вопросы.
2. Оценка «хорошо»: выполнены все индивидуальные задания по курсу, но срок их выполнения нарушался; продемонстрировано знание материла курса в целом, но были ошибки при ответе на вопрос билета или дополнительные вопросы, или в решениях задач из билета (экзаменуемый смог их исправить после наводящих вопросов преподавателя).
3. Оценка «удовлетворительно»: имеются невыполненные индивидуальные задания по курсу, но на экзамене решены задачи на соответствующие им темы; при ответе на вопросы билета и дополнительные вопросы обнаружено недостаточное знание ряда тем.
4. Оценка «неудовлетворительно»: не выполнены условия получения оценки «удовлетворительно».

**3.1.4 Методические материалы для проведения текущего контроля успеваемости и промежуточной аттестации (контрольно-измерительные материалы, оценочные средства)**

Примерный краткий перечень вопросов к экзамену:

1. Корректирующие коды. Примеры блочных кодов.
2. Линейные коды над GF(2).
3. Циклические коды.
4. Совершенные коды.
5. Коды Рида-Маллера 1-го порядка
6. Коды Рида-Маллера 2-го порядка.
7. Матрицы Адамара и методы их построения.

**3.1.5 Методические материалы для оценки обучающимися содержания и качества учебного процесса**

Оценка обучающимися содержания и качества учебного процесса по дисциплине осуществляется в установленном в СПбГУ порядке.

**3.2. Кадровое обеспечение**

**3.2.1 Образование и (или) квалификация штатных преподавателей и иных лиц, допущенных к проведению учебных занятий**

К чтению лекций и проведению семинаров привлекаются преподаватели, имеющие базовое образование и/или ученую степень, соответствующую профилю преподаваемой дисциплины.

**3.2.2 Обеспечение учебно-вспомогательным и (или) иным персоналом**

Не требуется.

**3.3. Материально-техническое обеспечение**

**3.3.1 Характеристики аудиторий (помещений, мест) для проведения занятий**

Стандартно оборудованные лекционные аудитории для проведения интерактивных занятий: видеопроектор, экран, др. оборудование.

**3.3.2 Характеристики аудиторного оборудования, в том числе неспециализированного компьютерного оборудования и программного обеспечения общего пользования, в том числе неспециализированного компьютерного оборудования и программного обеспечения общего пользования**

Нет

**3.3.3 Характеристики специализированного оборудования**

Не требуется.

**3.3.4 Характеристики специализированного программного обеспечения**

При использовании электронных документов каждый обучающийся во время самостоятельной подготовки должен быть обеспечен рабочим местом в компьютерном классе с выходом в Интернет и корпоративную сеть факультета.

**3.3.5 Перечень и объёмы требуемых расходных материалов**

Фломастеры цветные, губки, бумага формата А3 (для блокнота-доски), канцелярские товары в объеме, необходимом для организации и проведения занятий по заявкам преподавателей, подаваемым в установленные сроки, доступ преподавателя и студентов к в компьютерные классы.

**3.4. Информационное обеспечение**

**3.4.1 Список обязательной литературы**

1. Вернер М. Основы кодированияя. –М.: Техносфера, 2006. (Электронная версия http://www.studmed.ru/verner-m-osnovy-kodirovaniya\_f2159309178.html) .

2.Кудряшов Б.Д. Теория информации. Учебник для вузов. – СПб, ПИТЕР, 2008. (Электронная версия <http://window.edu.ru/resource/746/72746>).

3. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. – М.: Техносфера, 2006. (Электронная версия <http://mexalib.com/view/1731>).

4. Yuan Jiang, A Practical Guide to Error-Control Coding Using MATLAB, Boston&London, Artech House, 2010.( Электронная версия http://www.ebooks-share.net/a-practical-guide-to-error-control-coding-using-matlab/).

**3.4.2 Список дополнительной литературы**

1. Берлекэмп Э. Алгебраическая теория кодирования. − М.: Мир, 1971.

2. Блейхут Р. Теория и практика кодов, контролирующих ошибки. – М.: Мир, 1986.

3. Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А. Теория кодов, исправляющих ошибки. – М.: «Связь», 1979.

4. Ромащенко А.Е., Румянцев А.Ю., Шень А. Заметки по теории кодирования. – М.:МЦНМО, 2011.

5. Carlet C. Boolean Functions for Cryptography and Error Correcting Codes. – Cambridge University Press, 2010.

**3.4.3 Перечень иных информационных источников**

Не требуется.

**Раздел 4. Разработчики программы**

Агафонова Ирина Витальевна, доцент мат-мех факультета СПбГУ. i.agafonova@spbu , тел. 428-42-33.