Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Оренбургский государственный университет»

О.А. Пихтилькова, А.Н. Благовисная, Д.У. Шакирова

КУРСОВАЯ РАБОТА ПО ДИСЦИПЛИНЕ «ЛИНЕЙНЫЕ РЕКУРРЕНТЫ В КОНЕЧНЫХ ПОЛЯХ»

Методические указания

Рекомендовано к изданию редакционно-издательским советом федерального государственного бюджетного образовательного учреждения высшего образования «Оренбургский государственный университет» для обучающихся по образовательной программе высшего образования по направлению подготовки 02.04.01 Математика и компьютерные науки

Оренбург
2018

УДК 378.016:512.5(076.5)
ББК 22.14я7+74.48я7
П 35

Рецензент – доцент, кандидат физико-математических наук С.А. Герасименко

Пихтилькова, О.А.

П 35 Курсовая работа по дисциплине «Линейные рекурренты в конечных полях»: методические указания / О.А. Пихтилькова, А.Н. Благовисная, Д.У. Шакирова; Оренбургский гос. ун-т. – Оренбург: ОГУ, 2018. – 25 с.

Методические указания содержат основные рекомендации и требования по выполнению курсовых работ по дисциплине «Линейные рекурренты в конечных полях».

Методические указания составлены в соответствии с рабочей программой дисциплины «Линейные рекурренты в конечных полях» для обучающихся по направлению подготовки 02.04.01 Математика и компьютерные науки.

УДК 378.016:512.5(076.5)
ББК 22.14я7+74.48я7

Содержание

1 Общие положения

Курсовая работа по дисциплине «Линейные рекурренты в конечных полях» – вид самостоятельной письменной работы, направленный на творческое освоение дисциплины и выработку соответствующих профессиональных компетенций. При написании курсовой работы студент должен полностью раскрыть выбранную тему, соблюсти логику изложения материала, показать умение делать обобщения и выводы. Курсовая работа является одним из основных видов промежуточной аттестации и оценивает результаты учебной деятельности студента**.** Целью курсовой работы является углубление и расширение теоретических знаний и практических умений студента по учебной дисциплине. Смысл курсовой работы состоит в приобретении навыков самостоятельного решения практических проблем с научных позиций и письменного изложения полученных результатов.

Курсовая работа по дисциплине «Линейные рекурренты в конечных полях» включает в себя обязательную разработку программного продукта. Исключение составляют случаи, когда тема предполагает проведение математических доказательств, предложение и обоснование новых методик для решения задач криптографической защиты информации, проведение комплексного анализа существующих методов решения задач теории линейных рекуррентных последовательностей и других теоретических профессиональных задач.

Курсовая работа включает оформление пояснительной записки, рекомендуемая структура которой следующая:

- цели и задачи работы, объект и методы исследования;
- описание теоретических сведений, на основании которых разрабатывается программный продукт;
- описание пользовательских и технических характеристик программы;
- решение исследовательских задач, для которых программное средство разработано.

Примерный объем работы – 20-35 страниц.

2 О выборе темы курсовой работы

Тема курсовой работы либо выбирается студентом самостоятельно из примерного перечня тем, либо предлагается инициативная тема с обоснованием её выбора. В любом случае важно, чтобы тема была интересна студенту. В то же время необходимо адекватно оценивать возможности реализации выбираемой темы. Также рекомендуется выбирать тему таким образом, чтобы в дальнейшем материалы и результаты курсовой работы можно было использовать при написании выпускной квалификационной работы.

Прежде чем утверждать тему, необходимо убедиться, что доступен необходимый материал для ее раскрытия: студенту стоит произвести предварительный библиографический поиск в Интернете, в каталоге библиотеки и электронных базах университета, которые он будет реально посещать и к которым имеет доступ, соответственно. Кроме того, рекомендуется проконсультироваться с преподавателем, осуществляющим руководство курсовыми работами, по вопросу поиска материалов по теме.

3 Методика работы студента над курсовой работой

Практическое выполнение курсовой работы должно начинаться с планирования. Основой для этого планирования являются тема работы и задание руководителя, содержащее перечень основных вопросов, подлежащих разработке. На их основе разрабатывается календарный план выполнения работы, устанавливающий логическую последовательность, очередность и сроки завершения отдельных этапов работы. Календарный план должен предусматривать время на отбор всей необходимой информации, её изучение, обработку, оформление работы.

Кроме календарного плана студент должен иметь план, раскрывающий содержание курсовой работы. Возможны несколько вариантов такого плана. Первый вариант плана может носить предварительный характер, в дальнейшем он может изменяться, отдельные разделы могут быть расширены, конкретизированы, уточнены, представлены в новых формулировках.

В качестве примера приведем примерный план курсовой работы на тему «Методы усложнения линейных рекуррент на основе фильтрующих и комбинирующих генераторов».

Введение (характеристика состояния рассматриваемой проблемы, обоснование выбора темы, определение объекта и предмета исследования, формулировка цели и задач исследования).

1 Теоретические основы усложнения линейных рекуррент

1.1 Обзор литературы по теме иследования

1.2 Основные понятия и определения теории линейных рекуррентных последовательностей

1.3 Фильтрующие генераторы

1.4 Комбинирующие генераторы

1.5 Криптографические булевы функции

2 Реализация алгоритмов усложнения линейных рекуррентных последовательностей

2.1 Описание алгоритмов генерации булевых функций с криптографическими свойствами

2.2 Описание алгоритма, реализующего фильтрующие генераторы

2.3 Описание алгоритма, реализующего комбинирующие генераторы

2.4 Обоснование выбора языка и среды программирования

2.5 Описание программного средства, реализующего фильтрующие и кобинирующие генераторы

3 Сравнение реализованных алгоритмов усложнения линейных рекуррентных последовательностей

3.1 Сравнение фильтрующих генераторов в зависимости от криптографических характеристик булевых функций

3.2 Сравнение комбинирующих генераторов в зависимости от криптографических характеристик булевых функций

3.3 Сравнительный анализ фильтрующих и комбинирующих генераторов

Заключение

Список использованных источников

Приложение А Код программы, реализующей фильтрующий и комбинирующий генераторы

Опыт показывает, что название темы, план работы, перечень литературы ещё не определяют содержание темы. Здесь допустим широкий произвол в отборе материала, его объеме, методике изложения, реализации программного средства, выборе и постановке исследовательских задач, для решения которых используется программное средство. Именно это придает каждой работе индивидуальность, оригинальность, что позволяет судить об уровне теоретической и практической подготовленности автора.

Работа над темой начинается с отбора и изучения литературы (учебники, учебные пособия, монографии, статьи, Интернет-ресурсы). Первоначально надо

лишь в общих чертах ознакомиться с содержанием основных источников. При этом важен порядок изучения основных литературных источников. В большинстве случаев нужно начинать со знакомства с работами более общего характера, а затем переходить к изучению литературы, в которой излагаются детально конкретные вопросы.

Поиск информации является одной из важных компетенций студента. Для успешного поиска рекомендуется первоначально выделить основные термины, ключевые слова, фамилии ученых, касающиеся темы исследований.

После изучения литературы необходимо перейти к систематизации и анализу изученного материала, установлению логических связей и построению цельного изложения рассматриваемой темы. Курсовая работа носит исследовательский характер, поэтому в ней должно быть отражено проведение студентом самостоятельного научного поиска.

Основной этап выполнения сильно зависит от выбранной темы исследования и имеет большое количество форм. Так, в случае теоретического исследования, этот этап связан с анализом и систематизацией собранного научного материала, выявлением и анализом основных тенденций, закономерностей в исследуемой области, формулировкой и доказательством (обоснованием) теоретических положений. В случае эмпирического исследования создается программный продукт и с его помощью проводится вычислительный эксперимент.

Следующим этапом является оформление работы в виде пояснительной записки. Пояснительной запиской считается текст, включающий в себя полное теоретическое и практическое описание решаемых задач курсовой работы. Пояснительная записка оформляется в соответствии с требованиями, изложенными в разделе 5 данных методических указаний. Заметим, что, несмотря на то, что концептуальный состав пояснительной записки сильно зависит от темы выполненной курсовой работы, в тексте должны быть отражены ответы на следующие вопросы:

– что сделано?

– как сделано?

– что получилось в результате?

Заключительным этапом является защита курсовой работы. Для защиты необходимо представить доклад и презентацию выполненной курсовой работы, а также подготовиться к ответам на вопросы, которые могут возникнуть в процессе её обсуждения. При подготовке доклада и презентации для выступления студент должен иметь в виду следующие моменты. Ориентировочное время доклада – 5-7 минут. За время доклада необходимо обязательно сказать об актуальности выбранной темы, применяемых методах решения и описать результат, который был получен в работе. Доклад должен иметь целостный вид, чтобы создать законченное представление об актуальности, сложности и объеме выполненной работы. Большую часть времени доклада нужно посвятить собственным результатам и достижениям. Презентация должна дополнять доклад, а не быть отдельным элементом представления работы. Количество слайдов презентации в большинстве случаев не должно превышать 15. Текст в презентации должен быть представлен кратко, в виде основных тезисов. После завершения доклада следуют ответы студента на вопросы. Ответы на вопросы являются важным критерием оценивания выполненной работы, поэтому необходимо продумать заранее стратегию ответов.

4 Список тем курсовых работ

Далее приводятся примерные формулировки тем курсовых работ, а также список литературы, с которого рекомендуется начинать знакомство с выбранной темой.

Тема 1. Рекуррентные последовательности с большим периодом и их приложения в криптографии.

Литература для первоначального знакомства с темой:

1. Глухов, М. М. Алгебра: учебник в 2-х томах. Том II / М. М. Глухов, В. П. Елизаров, А. А. Нечаев. – М.: Гелиос АРВ, 2003. – 416 с.

2. Поточные шифры. Результаты зарубежной открытой криптологии. – Москва, 1997. – 389 с.

3. Карпов, А. В. Имитационная компьютерная модель криптографической системы, основанная на генераторах М-последовательности: учебно-методическое пособие / А. В. Карпов, И. Р. Туктарова, А. Д. Смоляков. – Казанский гос. ун-т. – Казань: Казанский университет, 2015. – 35 с.

4. Власов, Е. Г. Конечные поля в телекоммуникационных приложениях / Е. Г. Власов. – М.: ИНФРА-М, 2016. – 285 с.

5. Кузьмин, Н. А. Периоды разрядных последовательностей линейных рекуррент максимального периода над конечными простыми полями / Н. А. Кузьмин // Прикладная дискретная математика. – 2015. – № 1(27). – С. 62-68.

Тема 2. Исследование модификаций алгоритма Берлекэмпа-Месси.

Литература для первоначального знакомства с темой:

1. Алферов, А. П. Основы криптографии / А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин. – М.: Гелиос АРВ, 2002. – 480 с.

2. Блейхут, Р. Теория и практика кодов, контролирующих ошибки / Р. Блейхут. – М.: Мир, 1986. – 576 с.

3. Блейхут, Р. Быстрые алгоритмы цифровой обработки сигналов / Р. Блейхут. – М.: Мир, 1989. – 448 с.

4. Куракин, В.Л. Алгоритм Берлекэмпа-Месси над конечными кольцами, модулями и бимодулям / В. Л. Куракин // Дискретная математика. – 1998. – Т. 10. – № 4. – С. 3-34.

5. Хусаинов, Р. Н. Разработка программной реализации алгоритма Берлекэмпа-Месси для анализа и синтеза рекуррентных двоичных последовательностей / Р. Н. Хусаинов, М. Д. Галимов, Б. Ф. Эминов, А. И. Крюков // Вестник технологического университета. – 2015. – Т.18. – №24. – С. 89-91.

Тема 3. Построение криптографических булевых функций на основе линейных рекуррент.

Литература для первоначального знакомства с темой:

1. Отрыванкина, Т. М. Криптографические свойства булевых функций: методические указания / Т. М. Отрыванкина, А. Н. Благовисная; Оренбургский гос. ун-т. – Оренбург: ОГУ, 2014. – 55 с.

2. Логачев, О.А. Булевы функции в теории кодирования и криптологии / О. А. Логачев, А. А. Сальников, В. В. Ященко. – М.: МЦНМО, 2012. – 583 с.

3. Панкратова, И. А. Булевы функции в криптографии: учебное пособие / И. А. Панкратова. – Томск: Издательский дом Томского государственного университета, 2014. – 88 с.

4. Токарева, Н. Н. Симметричная криптография. Краткий курс: учебное пособие / Н. Н. Токарева. – Новосибирский государственный университет, Новосибирск, 2012. – 234 с.

5. Былков, Д. Н. Параметры булевых функций, построенных с использованием страших координатных последовательностей линейных рекуррент / Д. Н. Былков, О. В. Камловский // Математические вопросы криптографии. – 2012. – Т. 3. – №4. – С. 25-53.

6. Былков, Д. Н. Об одном классе булевых функций, построенных с использованием старших разрядных последовательностей линейных рекуррент /

Д. Н. Былков // Прикладная дискретная математика. Приложение. – 2014. – № 7. – С. 59–60.

7. Камловский, О. В. Нелинейность одного класса булевых функций, построенных с использованием двоичных разрядных последовательностей линейных рекуррент над кольцом Z_{2^n} / О. В. Камловский // Математические вопросы криптографии. – 2016. – Т. 7. – № 3. – С. 29–46.

Тема 4. Исследование и реализация моделей генераторов линейных рекуррентных последовательностей над конечными полями.

Литература для первоначального знакомства с темой:

1. Глухов, М. М. Алгебра: учебник в 2-х томах. Том II / М. М. Глухов, В. П. Елизаров, А. А. Нечаев. – М.: Гелиос АРВ, 2003. – 416 с.

2. Чугунков, И. В. Методы и средства оценки качества генераторов псевдослучайных последовательностей, ориентированных на решение задач защиты информации: учебное пособие / И. В. Чугунков. – М.: НИЯУ МИФИ, 2012. – 236 с.

3. Поточные шифры. Результаты зарубежной открытой криптологии. – Москва, 1997. – 389 с.

4. Власов, Е. Г. Конечные поля в телекоммуникационных приложениях / Е. Г. Власов. – М.: ИНФРА-М, 2016. – 285 с.

Тема 5. Исследование моделей генераторов ключевых последовательностей, основанных на регистрах сдвига.

Литература для первоначального знакомства с темой:

1. Алферов, А. П. Основы криптографии / А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин. – М.: Гелиос АРВ, 2002. – 480 с.

2. Поточные шифры. Результаты зарубежной открытой криптологии. – Москва, 1997. – 389 с.

3. Кузнецов, В. М. Генераторы равновероятностных псевдослучайных последовательностей на регистрах сдвига / В. М. Кузнецов, В. А. Песошин //

Известия высших учебных заведений. Поволжский регион. Технические науки. – 2012. – № 1 (21). – С. 21–28.

Тема 6. Реализация атаки на поточный шифр с использованием алгоритма Берлекэмпа-Месси.

Литература для первоначального знакомства с темой:

1. Алферов, А.П. Основы криптографии / А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин. – М.: Гелиос АРВ, 2002. – 480 с.

2. Логачев, О. А. Булевы функции в теории кодирования и криптологии / О. А. Логачев, А. А. Сальников, В. В. Ященко. – М.: МЦНМО, 2012. – 583 с.

3. Токарева, Н. Н. Симметричная криптография. Краткий курс: учебное пособие / Н. Н. Токарева. – Новосибирский государственный университет, Новосибирск, 2012. – 234 с.

Тема 7. Исследование методов усложнения линейных рекуррент.

Литература для первоначального знакомства с темой:

1. Алферов, А. П. Основы криптографии / А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин. – М.: Гелиос АРВ, 2002. – 480 с.

2. Логачев, О. А. Булевы функции в теории кодирования и криптологии / О. А. Логачев, А. А. Сальников, В. В. Ященко. – М.: МЦНМО, 2012. – 583 с.

3. Токарева, Н. Н. Симметричная криптография. Краткий курс: учебное пособие / Н. Н. Токарева. – Новосибирский государственный университет, Новосибирск, 2012. – 234 с.

4. Былков, Д. Н. Построение новых классов фильтрующих генераторов, не имеющих эквивалентных состояний / Д. Н. Былков // Математические вопросы криптографии. – 2014. – Т. 5. – №4. – С. 17–39.

Тема 8. Выбор криптографически стойких усложняющих функций для фильтрующих криптографических генераторов.

Литература для первоначального знакомства с темой:

1. Отрыванкина, Т. М. Криптографические свойства булевых функций: методические указания / Т. М. Отрыванкина, А. Н. Благовисная; Оренбургский гос. ун-т. – Оренбург: ОГУ, 2014. – 55 с.

2. Логачев, О. А. Булевы функции в теории кодирования и криптологии / О. А. Логачев, А. А. Сальников, В. В. Ященко. – М.: МЦНМО, 2012. – 583 с.

3. Панкратова, И. А. Булевы функции в криптографии: учебное пособие / И. А. Панкратова. – Томск: Издательский дом Томского государственного университета, 2014. – 88 с.

4. Токарева, Н. Н. Симметричная криптография. Краткий курс: учебное пособие / Н. Н. Токарева. – Новосибирский государственный университет, Новосибирск, 2012. – 234 с.

5. Алферов, А. П. Основы криптографии / А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин. – М.: Гелиос АРВ, 2002. – 480 с.

6. Поточные шифры. Результаты зарубежной открытой криптологии. – Москва, 1997. – 389 с.

Тема 9. Выбор криптографически стойких усложняющих функций для комбинирующих криптографических генераторов.

Литература для первоначального знакомства с темой:

1. Отрыванкина, Т. М. Криптографические свойства булевых функций: методические указания / Т. М. Отрыванкина, А. Н. Благовисная; Оренбургский гос. ун-т. – Оренбург: ОГУ, 2014. – 55 с.

2. Логачев, О. А. Булевы функции в теории кодирования и криптологии / О. А. Логачев, А. А. Сальников, В. В. Ященко. – М.: МЦНМО, 2012. – 583 с.

3. Панкратова, И. А. Булевы функции в криптографии: учебное пособие / И. А. Пакраторва. – Томск: Издательский дом Томского государственного университета, 2014. – 88 с.

4. Токарева, Н. Н. Симметричная криптография. Краткий курс: учебное пособие / Н. Н. Токарева. – Новосибирский государственный университет, Новосибирск, 2012. – 234 с.

5. Алферов, А. П. Основы криптографии / А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин. – М.: Гелиос АРВ, 2002. – 480 с.

6. Поточные шифры. Результаты зарубежной открытой криптологии. – Москва, 1997. – 389 с.

Тема 10. Реализация генератора гаммы с неравномерным движением.

Литература для первоначального знакомства с темой:

1. Алферов, А. П. Основы криптографии / А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин. – М.: Гелиос АРВ, 2002. – 480 с.

2. Поточные шифры. Результаты зарубежной открытой криптологии. – Москва, 1997. – 389 с.

Тема 11. Полилинейные рекурренты и их приложения.

Литература для первоначального знакомства с темой:

1. Кузьмин, А. С. Псевдослучайные и полилинейные последовательности / А. С. Кузьмин, В. Л. Куракин, А. А. Нечаев // Труды по дискретной математике. – 1997. – Т. 1. – С. 139–202.

2. Кузьмин, А. С. Свойства линейных и полилинейных рекуррент над кольцами Галуа (I) / А. С. Кузьмин, В. Л. Куракин, А. А. Нечаев // Труды по дискретной математике. – 1998. – Т. 2. – С. 191–222.

3. Кузьмин, А. С. Свойства линейных и полилинейных рекуррент над кольцами Галуа (II) / А. С. Кузьмин, В. Л. Куракин, А. А. Нечаев // Обозрение прикладной и промышленной математики. – 2000. – Т. 7. – №1. – С. 5–59.

4. Михалев, А. В. Цикловые типы семейств полилинейных рекуррент и датчики псевдослучайных чисел / А. В. Михалев, А. А. Нечаев // Математические вопросы криптографии. – 2014. – Т. 5. – № 1. – С. 95–125.

Тема 12. Линейные рекуррентные последовательности на эллиптических кривых.

Литература для первоначального знакомства с темой:

1. Болотов, А. А. Элементарное введение в эллиптическую криптографию: Протоколы криптографии на эллиптических кривых / А. А. Болотов, С. Б. Гашков, А. Б. Фролов. – М.: КомКнига, 2006. – 280 с.

2. Тараканов, В. Е. Линейные рекуррентные последовательности на эллиптических кривых и их применения в криптографии / В. Е. Тараканов // Труды по дискретной математике. – 2007. – № 10 . – С. 301-313.

3. Червяков, Н.И. Линейные рекуррентные последовательности на эллиптической кривой / Н.И. Червяков, М.Г. Бабенко // Научно-технические ведомости СПбГТУ. – 2010. – № 2. – С. 164-166.

Тема 13. Алгоритм А5 и его модификации.

Литература для первоначального знакомства с темой:

1. Алферов, А.П. Основы криптографии / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. – М.: Гелиос АРВ, 2002. – 480 с.

2. Логачев, О.А. Булевы функции в теории кодирования и криптологии / О.А. Логачев, А.А. Сальников, В.В. Ященко. – М.: МЦНМО, 2012. – 583 с.

3. Токарева, Н.Н. Симметричная криптография. Краткий курс: учебное пособие / Н.Н. Токарева. – Новосибирский государственный университет, Новосибирск, 2012. – 234 с.

4. Нечаев, Ю. Б. Защищенная связь в стандарте GSM / Ю. Б. Нечаев, Б. Н. Воронков, Е. С. Долбилова, А. В. Дудченко // Вестник ВГУ, серия: Системный анализ и информационные технологии. – 2006. – № 2. – С. 74-79.

Тема 14. Статистические методы оценки качества криптографических последовательностей.

Литература для первоначального знакомства с темой:

1. Поточные шифры. Результаты зарубежной открытой криптологии. – Москва, 1997. – 389 с.

2. Чугунков, И. В. Методы и средства оценки качества генераторов псевдослучайных последовательностей, ориентированных на решение задач защиты информации: учебное пособие / И. В. Чугунков. – М.: НИЯУ МИФИ, 2012. – 236 с.

Тема 15. Линейный конгруэнтный генератор и его модификации.

Литература для первоначального знакомства с темой:

1. Поточные шифры. Результаты зарубежной открытой криптологии. – Москва, 1997. – 389 с.

2. Чугунков, И. В. Методы и средства оценки качества генераторов псевдослучайных последовательностей, ориентированных на решение задач защиты информации: учебное пособие / И. В. Чугунков. – М.: НИЯУ МИФИ, 2012. – 236 с.

3. Герловина, В. М. О модификации метода распараллеливания ЛКГ / В. М. Герловина // Вестник Санкт-Петербургского университета. Сер. 10. – 2009. – Вып. 4. – С. 48-54.

5 Структура и оформление курсовой работы

При оформлении курсовой работы следует выдержать общие правила оформления, требования к текстовым документам, использование формул, таблиц, рисунков, сносок и других элементов, изложенные в «СТО 02069024.101–2015 РАБОТЫ СТУДЕНЧЕСКИЕ. Общие требования и правила оформления». Стандарт можно найти на официальном сайте Оренбургского государственного университета по ссылке http://www.osu.ru/docs/official/standart/standart_101-2015_.pdf.

Обязательными составляющими курсовой работы являются:

- титульный лист;
- содержание;
- введение;
- основная часть;
- заключение;
- список литературы.

Дополнительными составляющими курсовой работы являются:

- вспомогательные указатели;
- приложения.

Охарактеризуем обязательные и дополнительные составляющие курсовой работы.

Титульный лист является первой страницей курсовой работы и должен содержать следующие сведения: наименование учреждения (учебного заведения), название (тему), сведения о выполнившем курсовую работу, сведения о руководителе, наименование места и год выполнения.

Содержание включает перечень основных элементов курсовой работы с указанием номеров страниц, с которых начинается их месторасположение.

Введение содержит актуальность рассматриваемой темы, цель и задачи курсовой работы, объект и предмет исследования, особенности курсовой работы и основное смысловое содержание ее разделов.

После формулировки цели предпринимаемого исследования, следует указать конкретные задачи, которые предстоит решать в соответствии с этой целью. Это обычно делается в форме перечисления (изучить, описать, установить, выявить, вывести формулу, разработать и т.п.). Формулируя задачи, следует учитывать, что описание их решения должно составить содержание глав курсовой работы.

В конце введения желательно раскрыть структуру работы, то есть дать перечень ее структурных элементов и обосновать последовательность их расположения.

Чтобы осветить состояние разработки выбранной темы, составляется краткий обзор литературы. Обзор литературы может быть размещен как во введении, так и в первой главе работы, составляющей теоретическую основу исследования.

Обзор литературы по теме должен показать знакомство студента со специальной литературой, его умение систематизировать источники, выделять существенное, оценивать ранее сделанное другими исследователями, определять главное в современном состоянии изученности темы. Обзор работ следует делать только по вопросам выбранной темы, а не по всей проблеме в целом. В обзор включается только та литература, с которой студент ознакомился (знаком) лично.

Основная часть должна содержать текстовые материалы и данные, отражающие существо, методику и отдельные результаты, достигнутые в ходе выполнения курсовой работы. Материал основной части рекомендуется делить на главы, параграфы, пункты и подпункты. Такое деление должно способствовать более стройному и упорядоченному изложению материала. При этом каждый пункт должен содержать законченную информацию, логически вписывающуюся в общую структуру работы и способствующую достижению ее целей.

В заключении раскрывается значимость рассмотренных вопросов для теории и практики; приводятся выводы, характеризующие итоги проделанной работы, предложения и рекомендации.

Список литературы – это упорядоченный в алфавитной или хронологической последовательности перечень библиографических описаний документальных

источников информации по теме курсовой работы. В списке следует указывать авторов, наименование источника, издательство, год издания, количество страниц.

В состав вспомогательных указателей могут входить:

– список сокращений (оформляется в виде алфавитного перечня принятых в курсовой работе сокращений и соответствующих им полных обозначений понятий);

– список условных обозначений (оформляется в виде перечня используемых в тексте курсовой работы условных обозначений с соответствующей расшифровкой);

– указатель таблиц и иллюстраций (оформляется в виде перечня названий таблиц или иллюстраций, упорядоченных в соответствии с их порядковыми номерами, с указанием страниц их месторасположения в тексте курсовой работы).

Приложения помещаются в конце курсовой работы. Каждое приложение должно начинаться с новой страницы и иметь содержательный заголовок. Приложения должны иметь общую с остальной частью курсовой работы нумерацию страниц. На все приложения в основной части курсовой работы должны быть ссылки.

6 Защита курсовой работы

Выполненная курсовая работа сдается студентом руководителю в установленный срок. Руководитель знакомится с текстом курсовой работы, определяет её сильные и слабые стороны, проверяет работу в системе Антиплагиат, ставит предварительную оценку. При необходимости работа может быть возвращена студенту на доработку.

Курсовые работы, удовлетворяющие всем необходимым требованиям, допускаются к защите. Во время защиты докладчику дается возможность отстаивать и обосновывать свою точку зрения.

В презентации рекомендуется использовать не более 15 слайдов, которые нумеруются. Содержание слайдов не должно дублировать текст выступления. Оформление слайдов должно соответствовать требованиям эргономики.

На первом слайде сообщаются: фамилия и инициалы автора, название курсовой работы, фамилия и инициалы руководителя.

На следующих слайдах формулируются: объект и предмет, цели и задачи исследования; основные положения курсовой работы.

В конце презентации дается заключение, в котором должно быть сообщено о выполнении поставленных целей и задач.

Порядок обсуждения курсовой работы предусматривает ответы студента на вопросы преподавателей кафедры и других лиц, присутствующих на защите. Право выступать с замечаниями и пожеланиями имеют все присутствующие.

Решение об оценке курсовой работы принимается преподавателем кафедры, читающим лекции по дисциплине «Линейные рекурренты в конечных полях», по результатам анализа представленной курсовой работы, доклада студента и его ответов на вопросы. Оценка по итогам защиты курсовой работы проставляется в ведомость и зачетную книжку (с указанием темы) студента.

7 Критерии оценивания курсовой работы

Курсовая работа оценивается оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

При определении оценки знаний и умений, выявленных при защите курсовой работы, принимаются во внимание уровень теоретической, научной и практической подготовки студента.

Курсовая работа оценивается «отлично», если выполнены следующие требования:

– план курсовой работы соответствует её теме;

– содержание курсовой работы соответствует теме и плану курсовой работы;

– итоговая оценка оригинальности текста не менее 70%;

– основные понятия и теоремы рассмотрены полностью;

– изложенный материал структурирован;

– список использованной литературы состоит не менее чем из 15 источников, среди которых присутствуют публикации за последние 5 лет;

– выполнены требования «СТО 02069024.101–2015 РАБОТЫ СТУДЕНЧЕСКИЕ. Общие требования и правила оформления» (http://www.osu.ru/docs/official/standart/standart_101-2015_.pdf) к оформлению курсовой работы;

– отсутствуют орфографические и синтаксические ошибки, стилистические погрешности;

– курсовая работа сдана не позднее, чем за 10 дней до её защиты;

– защита курсовой работы выполнена по всем критериям, перечисленным далее.

Критерии защиты курсовой работы:

– количество слайдов соответствует содержанию и продолжительности выступления;

– наличие титульного слайда, слайда с формулировкой объекта, предмета, цели и задач курсовой работы, слайдов с выводами;

– иллюстрации хорошего качества, с четким изображением, текст легко читается;

– используются средства наглядности информации (таблицы, схемы, графики и т.д.)

– оформление слайдов соответствует теме, не препятствует восприятию содержания;

– для всех слайдов презентации используется один и тот же шаблон оформления;

– презентация содержит полную, понятную информацию по теме работы;

– презентация не содержит орфографических и пунктуационных ошибок;

– выступающий свободно владеет содержанием, ясно и грамотно излагает материал;

– выступающий свободно и корректно отвечает на вопросы и замечания аудитории;

– выступающий точно укладывается в рамки регламента.

Оценка «хорошо» ставится за курсовую работу, если не выполнены до 3 требований, перечисленных в критериях оценки «отлично».

Оценка «удовлетворительно» ставится за курсовую работу, если не выполнены до 5 требований, перечисленных в критериях оценки «отлично».

Оценка «неудовлетворительно» ставится за курсовую работу, если не выполнены 5 и более требований, перечисленных в критериях оценки «отлично».

8 Перечень рекомендуемых Интернет-ресурсов

Помимо библиотечных ресурсов, на современном этапе развития важным источником информации является Интернет. Существует масса открытых образовательных и научных порталов, концентрирующих в себе множество современных источников информации. Охарактеризуем Интернет-ресурсы, которые могут быть рекомендованы для написания курсовых работ по дисциплине «Линейные рекурренты в конечных полях».

В Оренбургском государственном университете имеется бесплатный для студентов доступ к электронным российским и зарубежным ресурсам. Познакомиться с актуальной информацией относительно перечня ресурсов и доступа к ним можно на сайте научной библиотеки Оренбургского государственного университета http://artlib.osu.ru/site_new/.

Полезную информацию для написания курсовой работы можно найти на следующих ресурсах:

1) http://eqworld.ipmnet.ru/indexr.htm (международный научно-образовательный сайт «Мир математических уравнений», который содержит обширную учебную физико-математическую библиотеку и предназначен для широкого круга ученых, преподавателей вузов, инженеров, аспирантов и студентов в различных областях математики и других наук; все ресурсы сайта являются бесплатными для его пользователей);

2) http://intuit.ru/ (сайт Национального Открытого Университета «ИНТУИТ»);

3) http://cryptography.ru/about/ (сайт посвящен вопросам математической криптографии, содержит календарь конференций, семинаров и т. п., которые полностью или частично посвящены вопросам защиты информации, а также актуальные ссылки на сайты данных научных мероприятий);

4) http://www.mathnet.ru/index.phtml/?option_lang=rus (общероссийский математический портал, современная информационная система, предоставляющая российским и зарубежным математикам различные возможности в поиске

информации о математической жизни в России);

5) https://arxiv.org/ (крупнейший бесплатный архив электронных публикаций научных статей и их препринтов по физике, математике, астрономии, информатике и биологии);

6) http://fstec.ru/ (Официальный сайт Федеральной службы по техническому и экспортному контролю. ФСТЭК России – федеральный орган исполнительной власти России, осуществляющий реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности).