МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Методические указания по выполнению практических работ по дисциплине
Математическое и программное обеспечение защиты информации

для студентов направления подготовки
01.04.02 Прикладная математика и информатика

Ставрополь, 2026

Содержание

Введение

Дисциплина «Математическое и программное обеспечение защиты информации» относится к ФТД.В.02 - ФТД. Факультативы. Часть, формируемая участниками образовательных отношений части учебного плана 2024 года и изучается студентами магистратуры специальности 01.04.02 направления «Прикладная математика и информатика» в 2 семестре.

Целью освоения дисциплины является изучить математическое и программное обеспечение защиты информации

Решаемые задачи:

1. Современные проблемы информационной безопасности.
2. Общесистемные аспекты криптологии. Основные понятия криптологии.
3. Модулярная арифметика.
4. Криптографические алгоритмы, симметричные шифры,
5. асимметричное шифрование, электронная цифровая подпись
5. криптографический алгоритм Рабина,
6. забывчивый протокол передачи данных,
7. доказательство с нулевым разглашением,
8. протокол Фиата-Шамира.

Формы отчетности: зачет - 2 семестр.

Содержание дисциплины: Современные проблемы информационной безопасности. Общесистемные аспекты криптологии. Основные понятия криптологии. Модулярная арифметика. Криптографические алгоритмы, симметричные шифры, асимметричное шифрование, электронная цифровая подпись, криптографиечский алгоритм Рабина, забывчивый протокол передачи данных, доказательство с нулевым разглашением, протокол Фиата-Шамира.

Реализуемые компетенции:

ПК-7 - Способен управлять информацией с использованием цифровых средств и алгоритмов обработки данных для решения задач профессиональной деятельности

Рекомендуемое программное обеспечение:

1. Математическая программная среда SciLab (версия не ниже 5.3)
2. Интегрированная среда разработки программ Lazarus (версия не ниже 1.4)
3. Операционная система: Windows , Linux (Mint не ниже 17.2)

Рекомендуемое материально-техническое обеспечение: компьютерный класс (лаборатория, аудитория) с числом исправных ЭВМ по числу студентов группы плюс рабочее место преподавателя и производительностью, достаточной для освоения дисциплины. На всех ЭВМ класса (лаборатории, аудитории) программное обеспечение, выход в интернет для изучения интернет-источников дисциплины (со скоростью доступа, достаточной для комфортной работы).

Практическая работа №1

Тема: «Современные проблемы информационной безопасности.»

Цель работы: «закрепление знаний по теоретическим основам современных проблем информационной безопасности».

Формируемые компетенции (формируется часть компетенций):

ПК-7 - Способен управлять информацией с использованием цифровых средств и алгоритмов обработки данных для решения задач профессиональной деятельности

Ход работы

1. Орг. момент.
2. Выбор задания в соответствие с вариантом.
3. Изучение теоретической части (литературы) по теме работы.
4. Изучение техники безопасности (правил поведения в компьютерной лаборатории).
5. Выполнение работы.
- загрузить шаблон программы.
- внести в шаблон необходимые изменения.
- отладить полученную компьютерную программу.
6. Оформление результатов работы.
7. Выводы по проделанной работе.
8. Защита работы.

Теоретическая часть

См. список рекомендуемой литературы.

Оборудование и материалы: см. приложение 1.

Техника безопасности: см. приложение 3.

Задания для практической работы

Разработать в соответствие с выбранным вариантом концептуальную криптомодель, провести этапы спецификации и наблюдений, продумать дальнейшие шаги общей схемы системного подхода

1. криптомодель генерации случайных и псевдослучайных чисел
2. криптомодель генерации абсолютно стойкого шифра Шеннона
3. криптомодель генерации ключей RSA
4. криптомодель генерации зашифрованного туннеля обмена сообщениями
5. криптомодель электронной подписи текстовых документов
6. криптомодель забывчивого протокола передачи информации
7. криптомодель аутентификации по протоколу Фиата-Шамира
8. криптомодель доказательства с нулевым разглашением
9. криптомодель шифрования/дешифрования на основе алгоритма Рабина
10. криптомодель оценки информационной безопасности компьютерной программы

Контрольные вопросы

1. Современные проблемы информационной безопасности.
2. Общесистемные аспекты криптологии. Основные понятия криптологии.
3. Модулярная арифметика.
4. Криптографические алгоритмы, симметричные шифры,
5. асимметричное шифрование, электронная цифровая подпись
5. криптографический алгоритм Рабина,
6. забывчивый протокол передачи данных,
7. доказательство с нулевым разглашением,
8. **протокол Фиата-Шамира.**

Список литературы, рекомендуемый к использованию по данной теме

Основная литература:

1. Червяков Н.И., Ляхов П.А., Копыткова Л.Б., Гладков А.В. Обработка информации в системе остаточных классов: Учебное пособие. – Ставрополь: СКФУ, 2016. – 182 с.
2. Червяков Н.И. и др. Модулярная арифметика и ее приложения в инфокоммуникационных технологиях / Под ред. Н.И.Червякова. – Москва : Физматлит, 2017. – 400 с.

Дополнительная литература

1. Червяков Н.И., Евдокимов А.А., Галушкин А.И., Лавриненко И.Н. Применение искусственных нейронных сетей и системы остаточных классов в криптографии. – М.: ФИЗМАТЛИТ, 2012. – 280 с.
2. Кочеров Ю.Н., Червяков Н.И. Разработка методов и алгоритмов разделения и восстановления данных в модулярных пороговых структурах для распределенных вычислительных сетей: монография / Ю. Н. Кочеров, Н. И. Червяков. – Ставрополь : СКФУ, 2016. – 239 с.
3. Введение в криптографию / [В. В. Ященко и др.] ; под ред. В. В. Ященко. - 3-е изд., испр. - М. : МЦНМО-ЧеРо, 2000. - 288 с.

Практическая работа №2

Тема: «Модулярная арифметика»

Цель работы: «закрепление знаний по теоретическим основам модулярной арифметики».

Формируемые компетенции (формируется часть компетенций):

ПК-7 - Способен управлять информацией с использованием цифровых средств и алгоритмов обработки данных для решения задач профессиональной деятельности

Ход работы

1. Орг. момент.
2. Выбор задания в соответствие с вариантом.
3. Изучение теоретической части (литературы) по теме работы.
4. Изучение техники безопасности (правил поведения в компьютерной лаборатории).
5. Выполнение работы.
- загрузить шаблон программы.
- внести в шаблон необходимые изменения.
- отладить полученную компьютерную программу.
6. Оформление результатов работы.
7. Выводы по проделанной работе.
8. Защита работы.

Теоретическая часть

См. список рекомендуемой литературы.

Оборудование и материалы: см. приложение 1.

Техника безопасности: см. приложение 3.

Задания для практической работы

Реализовать в соответствие с выбранным вариантом криптомодель, провести этапы идентификации и экспериментов, продумать дальнейшие шаги общей схемы системного подхода

1. криптомодель генерации случайных и псевдослучайных чисел
2. криптомодель генерации абсолютно стойкого шифра Шеннона
3. криптомодель генерации ключей RSA
4. криптомодель генерации зашифрованного туннеля обмена сообщениями
5. криптомодель электронной подписи текстовых документов
6. криптомодель забывчивого протокола передачи информации
7. криптомодель аутентификации по протоколу Фиата-Шамира
8. криптомодель доказательства с нулевым разглашением
9. криптомодель шифрования/дешифрования на основе алгоритма Рабина
10. криптомодель оценки информационной безопасности компьютерной программы

Контрольные вопросы

1. Современные проблемы информационной безопасности.
2. Общесистемные аспекты криптологии. Основные понятия криптологии.
3. Модулярная арифметика.
4. Криптографические алгоритмы, симметричные шифры,
5. асимметричное шифрование, электронная цифровая подпись
5. криптографический алгоритм Рабина,
6. забывчивый протокол передачи данных,
7. доказательство с нулевым разглашением,
8. протокол Фиата-Шамира.

Список литературы, рекомендуемый к использованию по данной теме

Основная литература:

1. Червяков Н.И., Ляхов П.А., Копыткова Л.Б., Гладков А.В. Обработка информации в системе остаточных классов: Учебное пособие. – Ставрополь: СКФУ, 2016. – 182 с.
2. Червяков Н.И. и др. Модулярная арифметика и ее приложения в инфокоммуникационных технологиях / Под ред. Н.И.Червякова. – Москва : Физматлит, 2017. – 400 с.

Дополнительная литература

1. Червяков Н.И., Евдокимов А.А., Галушкин А.И., Лавриненко И.Н. Применение искусственных нейронных сетей и системы остаточных классов в криптографии. – М.: ФИЗМАТЛИТ, 2012. – 280 с.
2. Кочеров Ю.Н., Червяков Н.И. Разработка методов и алгоритмов разделения и восстановления данных в модулярных пороговых структурах для распределенных вычислительных сетей: монография / Ю. Н. Кочеров, Н. И. Червяков. – Ставрополь : СКФУ, 2016. – 239 с.
3. Введение в криптографию / [В. В. Ященко и др.] ; под ред. В. В. Ященко. - 3-е изд., испр. - М. : МЦНМО-ЧеРо, 2000. - 288 с.

практическая работа №3

Тема: «Криптографические алгоритмы».

Цель работы: «закрепление знаний по теоретическим основам Криптографических алгоритмов».

Формируемые компетенции (формируется часть компетенций):

ПК-7 - Способен управлять информацией с использованием цифровых средств и алгоритмов обработки данных для решения задач профессиональной деятельности

Ход работы

1. Орг. момент.
2. Выбор задания в соответствие с вариантом.
3. Изучение теоретической части (литературы) по теме работы.
4. Изучение техники безопасности (правил поведения в компьютерной лаборатории).
5. Выполнение работы.
- загрузить шаблон программы.
- внести в шаблон необходимые изменения.
- отладить полученную компьютерную программу.
6. Оформление результатов работы.
7. Выводы по проделанной работе.
8. Защита работы.

Теоретическая часть

См. список рекомендуемой литературы.

Оборудование и материалы: см. приложение 1.

Техника безопасности: см. приложение 3.

Задания для практической работы

Оптимизировать в соответствие с выбранным вариантом криптомодель,

1. криптомодель генерации случайных и псевдослучайных чисел
2. криптомодель генерации абсолютно стойкого шифра Шеннона
3. криптомодель генерации ключей RSA
4. криптомодель генерации зашифрованного туннеля обмена сообщениями
5. криптомодель электронной подписи текстовых документов
6. криптомодель забывчивого протокола передачи информации
7. криптомодель аутентификации по протоколу Фиата-Шамира
8. криптомодель доказательства с нулевым разглашением
9. криптомодель шифрования/дешифрования на основе алгоритма Рабина
10. криптомодель оценки информационной безопасности компьютерной программы

Контрольные вопросы

1. Современные проблемы информационной безопасности.

2. Общесистемные аспекты криптологии. Основные понятия криптологии.
3. Модулярная арифметика.
4. Криптографические алгоритмы, симметричные шифры,
5. асимметричное шифрование, электронная цифровая подпись
5. криптографический алгоритм Рабина,
6. забывчивый протокол передачи данных,
7. доказательство с нулевым разглашением,
8. протокол Фиата-Шамира.

Список литературы, рекомендуемый к использованию по данной теме

Основная литература:

1. Червяков Н.И., Ляхов П.А., Копыткова Л.Б., Гладков А.В. Обработка информации в системе остаточных классов: Учебное пособие. – Ставрополь: СКФУ, 2016. – 182 с.
2. Червяков Н.И. и др. Модулярная арифметика и ее приложения в инфокоммуникационных технологиях / Под ред. Н.И.Червякова. – Москва : Физматлит, 2017. – 400 с.

Дополнительная литература

1. Червяков Н.И., Евдокимов А.А., Галушкин А.И., Лавриненко И.Н. Применение искусственных нейронных сетей и системы остаточных классов в криптографии. – М.: ФИЗМАТЛИТ, 2012. – 280 с.
2. Кочеров Ю.Н., Червяков Н.И. Разработка методов и алгоритмов разделения и восстановления данных в модулярных пороговых структурах для распределенных вычислительных сетей: монография / Ю. Н. Кочеров, Н. И. Червяков. – Ставрополь : СКФУ, 2016. – 239 с.
3. Введение в криптографию / [В. В. Ященко и др.] ; под ред. В. В. Ященко. - 3-е изд., испр. - М. : МЦНМО-ЧеРо, 2000. - 288 с.

Литература

Основная литература:

1. Червяков Н.И., Ляхов П.А., Копыткова Л.Б., Гладков А.В. Обработка информации в системе остаточных классов: Учебное пособие. – Ставрополь: СКФУ, 2016. – 182 с.
2. Червяков Н.И. и др. Модулярная арифметика и ее приложения в инфокоммуникационных технологиях / Под ред. Н.И.Червякова. – Москва : Физматлит, 2017. – 400 с.

Дополнительная литература

1. Червяков Н.И., Евдокимов А.А., Галушкин А.И., Лавриненко И.Н. Применение искусственных нейронных сетей и системы остаточных классов в криптографии. – М.: ФИЗМАТЛИТ, 2012. – 280 с.
2. Кочеров Ю.Н., Червяков Н.И. Разработка методов и алгоритмов разделения и восстановления данных в модулярных пороговых структурах для распределенных вычислительных сетей: монография / Ю. Н. Кочеров, Н. И. Червяков. – Ставрополь : СКФУ, 2016. – 239 с.
3. Введение в криптографию / [В. В. Ященко и др.] ; под ред. В. В. Ященко. - 3-е изд., испр. - М. : МЦНМО-ЧеРо, 2000. - 288 с.

Приложение 1.

Оборудование, материалы и программное обеспечение, используемые для организации и проведении практических работ

Оборудование:

Компьютерный класс (лаборатория, аудитория) с числом исправных ЭВМ по числу студентов группы плюс рабочее место преподавателя и производительностью, достаточной для освоения дисциплины.

Программное обеспечение:

4. Математическая программная среда SciLab (версия не ниже 5.3)
5. Интегрированная среда разработки программ Lazarus (версия не ниже 1.4)
6. Операционная система: Windows (версия не менее XP), Linux (Mint не ниже 17.2)

Приложение 2

Содержимое отчета по лабораторной работе

практическая работа считается выполненной студентом и засчитывается преподавателем (с зачислением баллов пропорционально выполненным пунктам отчета, т. е. необязательно, чтобы отчет содержал все пункты) при предоставлении в электронном виде к защите (бумажная распечатка не требуется!!!) аккуратно оформленного файла-отчета в формате .odt (OpenOffice, LibreOffice) или .doc (Microsoft Office), именованный по шаблону (при несоответствии работа не допускается к защите):

MPDD_MAG_LR(номер работы)_V(номер варианта)_(фамилия).odt

Файл-отчет должен иметь следующие элементы в указанном порядке (с сохранением их номера в случае пропуска некоторых пунктов):

0. Отметка об ознакомлении с техникой безопасности (правилами поведения в компьютерном классе (аудитории, лаборатории)).

В данном пункте необходимо наличие записи «С правилами техники безопасности при выполнении лабораторной работы и поведения в компьютерном классе (аудитории, лаборатории) ознакомлен, обязуюсь выполнять _____ (ФИО), _____ дата».

1. Постановка задачи (полное условие в соответствии с выбранным вариантом).

2. Подробная математическая (совокупность формул и поясняющего формулы текста) или информационной (словесное описание алгоритма) модели решения задачи. В данном пункте допустимо наличие экранных снимков расчетов в системах компьютерной алгебры (SciLab, Octave, Maxima и т.п.) или профессиональных графических системах. Использование проприетарных (коммерческих) систем (MathCad, MatLab и т.п.) не рекомендуется.

3. Тестовые наборы исходных данных и соответствующих им правильных результатов для проверки работоспособности программы (в данном пункте **должно быть ручное решение задачи с промежуточными выкладками**). В данном пункте допустимо наличие экранных снимков расчетов в системах компьютерной алгебры (SciLab, Octave, Maxima и т.п.) или профессиональных графических системах. Использование проприетарных (коммерческих) систем (MathCad, MatLab и т.п.) не рекомендуется.

4. Указание имен, типов и назначения всех переменных и сигналов, входящих в математическую или информационную криптомодель.

5. Основной и вспомогательные (если есть) алгоритмы решения задачи (допустимо описание алгоритма на алгоритмическом языке, например, Pascal).

6. Запись полных имен файлов, образующих проект с указанием назначения каждого файла (минимум указать имена и содержимое файлов).

7. Полные исходные тексты компьютерных программ (в каждом файле обязательно наличие информации о разработчике — ФИО, курс, группа, специальность, университет).

8. Экранный снимок или распечатка результата работы компьютерной программы при введенных тестовых данных из пункта 3 отчета. Конкретно в данном пункте необходимо сравнить полученные результаты с эталонным тестовым решением и написать «результат совпадает с эталонным решением».
9. Исследование проекта.
В данном пункте требуется записать несколько наборов входных данных (определить самостоятельно) и соответствующих им результатов. Оценить примерное число шагов и время работы алгоритма решения задачи в общем случае.
10. Выводы о проделанной работе.
Указать возможности, достоинства и недостатки, привести примеры использования.

Приложение 3

Правила поведения в компьютерном классе (аудитории, лаборатории)

1. К работе в компьютерном классе допускаются лица, ознакомленные с инструкцией по технике безопасности и охране труда, с правилами поведения и размещения информационных ресурсов.
2. Работа студентов в компьютерном классе разрешается только в присутствии преподавателя (инженера, лаборанта).
3. Во время групповых занятий посторонние лица могут находиться в классе только с разрешения преподавателя.
4. **Перед началом работы необходимо:**

– убедиться в отсутствии видимых повреждений на рабочем месте;
– разместить на столе тетради, учебные пособия так, чтобы они не мешали работе на компьютере;
– принять правильную рабочую позу;
– если сеанс работы предыдущего пользователя не был завершен, завершить его;
– ввести регистрационную информацию (при необходимости).

5. **При работе в компьютерном классе категорически запрещается:**

– находиться в классе в верхней одежде;
– размещать одежду и сумки на рабочих местах;
– находиться в классе с едой и напитками;
– класть книги, тетради и т.п. на клавиатуру;
– располагаться сбоку или сзади от включенного монитора;
– присоединять или отсоединять кабели, трогать разъемы, провода и розетки;
– передвигать компьютеры;
– открывать системный блок;
– пытаться самостоятельно устранять неисправности в работе аппаратуры;
– перекрывать вентиляционные отверстия на системном блоке и мониторе;
– ударять по клавиатуре, нажимать бесцельно на клавиши;
– удалять или перемещать чужие файлы;
– устанавливать и запускать компьютерные игры;
– использовать Интернет-ресурсы неучебного назначения.

6. **Находясь в компьютерном классе, необходимо:**

– соблюдать тишину и порядок, выключать мобильные телефоны от громкой связи;
– выполнять все требования преподавателя, инженера и лаборанта;
– работать только под своим именем и паролем;
– соблюдать режим работы (продолжительность непрерывной работы за компьютером не более двух часов с обязательным 10-минутным перерывом и

гимнастикой для глаз; продолжительность интенсивной работы с клавиатурой не более 30 минут с последующей гимнастикой для рук; общая продолжительность работы не более 4 часов в день);

– при появлении рези в глазах, резком ухудшении видимости, невозможности сфокусировать взгляд или навести его на резкость, появлении боли в пальцах и кистях рук, усилении сердцебиения немедленно покинуть рабочее место, сообщить о происшедшем преподавателю и обратиться к врачу;

– после окончания работы завершить все активные программы и корректно завершить сеанс;

– оставить рабочее место чистым.

7. **Работая за компьютером, необходимо соблюдать правильную позу:**

– расстояние от экрана до глаз 70-80 см (расстояние вытянутой руки);

– вертикально прямая спина;

– плечи опущены и расслаблены;

– ноги на полу и не скрещены;

– локти, запястья и кисти рук на одном уровне;

– локтевые, тазобедренные, коленные, голеностопные суставы под прямым углом.

8. При появлении программных ошибок или сбоях оборудования студент обязан немедленно обратиться к преподавателю (инженеру, лаборанту).

9. В случае порчи или выхода из строя оборудования компьютерного класса по вине пользователя ремонт или замена оборудования производится за счет пользователя.