Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования
Санкт-Петербургский горный университет

Кафедра информационных систем и вычислительной техники

УЧЕБНАЯ ПРАКТИКА – ОЗНАКОМИТЕЛЬНАЯ ПРАКТИКА – ПЕРВАЯ УЧЕБНАЯ ПРАКТИКА

Методические указания к первой учебной практике для студентов магистратуры направления 09.04.02

САНКТ-ПЕТЕРБУРГ
2021

УДК 004.4 (073)

УЧЕБНАЯ ПРАКТИКА – ОЗНАКОМИТЕЛЬНАЯ ПРАКТИКА – ПЕРВАЯ УЧЕБНАЯ ПРАКТИКА: Методические указания к первой учебной практике / Санкт-Петербургский горный университет. Сост. *В.Я. Трофимец*. СПб, 2021. 35 с.

Методические указания определяют цель, задачи, конкретное содержание, особенности организации и порядок прохождения первой учебной практики обучающимися, а также содержат требования по подготовке итогового отчета о практике.

Предназначены для студентов магистратуры подготовки 09.04.02 «Информационные системы и технологии», направленность (профиль) «Информационные системы и технологии».

Научный редактор доц. *Е.Б. Мазаков*

Рецензент к.ф.-м.н. *А.Н. Кривцов* (СПбГУТ им. проф. М.А. Бонч-Бруевича)

УЧЕБНАЯ ПРАКТИКА – ОЗНАКОМИТЕЛЬНАЯ ПРАКТИКА – ПЕРВАЯ УЧЕБНАЯ ПРАКТИКА

Методические указания к первой учебной практике для студентов магистратуры направления 09.04.02

Сост.: *В.Я. Трофимец*

Печатается с оригинал-макета, подготовленного кафедрой информационных систем и вычислительной техники

Ответственный за выпуск *В.Я. Трофимец*

Лицензия ИД № 06517 от 09.01.2002

Подписано к печати 29.04.2021. Формат 60×84/16.
Усл. печ. л. 2,0. Усл.кр.-отт. 2,0. Уч.-изд.л. 1,8. Тираж 75 экз. Заказ 375.

Санкт-Петербургский горный университет
РИЦ Санкт-Петербургского горного университета
Адрес университета и РИЦ: 199106 Санкт-Петербург, 21-я линия, 2

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Общая характеристика практики

Вид практики: учебная практика.

Тип практики: ознакомительная практика.

Форма практики: непрерывно – путем выделения в календарном учебном графике непрерывного периода учебного времени для проведения всех видов практик, предусмотренных ОПОП ВО.

Местом проведения учебной практики является специализированная лаборатория кафедры информационных систем и вычислительной техники Горного университета.

Учебная практика «Учебная практика – ознакомительная практика – Первая учебная практика» относится к обязательной части Блока 2 «Практика» основной профессиональной образовательной программы магистратуры по направлению подготовки 09.04.02 «Информационные системы и технологии», направленность (профиль) «Информационные системы и технологии» и проходит в 1 семестре.

Место практики в структуре ОПОП ВО – 1-й семестр. Объем практики – 2 з.е. ($1\,1/3$ недели).

1.2. Формируемые компетенции

Процесс прохождения учебной практики направлен на формирование следующих компетенций:

Формируемые компетенции		**Код и наименование индикатора достижения компетенции**
Содержание компетенции	**Код компетенции**	
Способен анализировать профессиональную информацию, выделять в ней главное, структурировать, оформлять и представлять в виде аналитических	ОПК-3	**ОПК-3.1. Знать:** принципы, методы и средства анализа и структурирования профессиональной информации; **ОПК-3.2. Уметь:** анализировать профессиональную информацию, выделять в ней главное, структурировать, оформлять и представлять в виде аналитических обзоров; **ОПК-3.3. Иметь навыки:** подготовки научных докладов, публикаций и аналитических

Формируемые компетенции		Код и наименование индикатора достижения компетенции
Содержание компетенции	**Код компетенции**	
обзоров с обоснованными выводами и рекомендациями		обзоров с обоснованными выводами и рекомендациями.
Способен осуществлять эффективное управление разработкой программных средств и проектов	ОПК-8	**ОПК-8.1. Знать:** методологии эффективного управления разработкой программных средств и проектов; **ОПК-8.2. Уметь:** планировать комплекс работ по разработке программных средств и проектов; **ОПК-8.3. Иметь навыки:** разработки программных средств и проектов в команде.

1.3. Структура и содержание практики

Общий объём практики составляет 2 зачетных единицы, что составляет 72 ак. часов. Вид промежуточной аттестации – дифференцированный зачет.

Этапы практики	Всего ак. часов	Ак. часы по семестрам
		1
Самостоятельная работа: в том числе	**72**	**72**
Подготовительный этап	4	4
Основной этап	56	56
Заключительный этап	12	12
Вид промежуточной аттестации дифф. зачет – (ДЗ)	**ДЗ**	**ДЗ**
Общая трудоемкость дисциплины:		
ак. час.	**72**	**72**
зач. ед.	**2**	**2**

Содержание разделов практики

№ п/п	Этапы практики	Виды работ на практике	Трудоёмкость в ак. часах
1.	Подготовительный этап	Инструктаж по технике безопасности, пожарной безопасности, охраны труда и правил внутреннего распорядка	1
		Проведение установочного семинара; постановка целей и задач на прохождение практики. Предварительное обсуждение постановки задачи, составление плана работы	3
			4
2.	Основной этап	Прохождение курса академии Cisco «Введение в кибербезопасность»	56
			56
3.	Заключительный этап	Подготовка отчета по практике	8
		Дифференцированный зачет	4
			12
		Итого:	**72**

1.4. Требования к содержанию учебной практики

Содержание учебной практики должно отвечать требованиям федерального государственного образовательного стандарта в части ознакомления студентов с видами будущей профессиональной деятельности (проектной, организационно-технологической, производственно-управленческой, научно-исследовательской и т. п.), формирования практических навыков и умений, приобретения опыта выполнения инженерных работ, давать представление о структурных подразделениях предприятия и основных технологических процессах, применении современных информационных технологий.

2. ОТЧЕТНОСТЬ ПО ПРАКТИКЕ

2.1. Форма отчетности

Формой отчетности по результатам прохождения учебной практики «Учебная практика – ознакомительная практика – Первая учебная практика» является отчет по практике.

Содержание отчета представляется в виде пояснительной записки (ПЗ), включающей собственно текст, таблицы, иллюстрации, формулы, уравнения и другие составляющие.

Завершенный отчет по учебной практике представляется студентом руководителю по практике.

Промежуточная аттестация по результатам учебной практики проводится в форме дифференцированного зачета.

2.2. Примерная структура отчета

1. Титульный лист
2. Содержание
3. Введение
4. Основная часть:

– краткое описание выполненных лабораторных работ по курсу академии Cisco «Введение в кибербезопасность»;

– представление результатов, формулировка выводов.

5. Заключение
6. Список использованных источников
7. Приложения

2.3. Требования по оформлению отчета

Отчет выполняется в текстовом редакторе MS Word. Шрифт Times New Roman (Cyr), кегль 12 пт, межстрочный интервал полуторный, отступ первой строки – 1,25 см; автоматический перенос слов; выравнивание – по ширине.

Используемый формат бумаги – А4, формат набора 165 × 252 мм (параметры полосы: верхнее поле – 20 мм; нижнее – 25 мм; левое – 30 мм; правое – 15 мм).

Стиль списка использованной литературы: шрифт – Times New Roman, кегль 12 пт, обычный. На все работы, приведенные в списке, должны быть ссылки в тексте пояснительной записки.

Иллюстрации: размер иллюстраций должен соответствовать формату набора – не более 165 × 252 мм. Подрисуночные подписи набирают, отступив от тела абзаца 0,5 см, основным шрифтом Times New Roman, кегль 11 пт, обычный.

Объем отчета должен содержать не менее 15-20 страниц печатного текста, включая приложения.

Текст отчёта делят на разделы, подразделы, пункты. Заголовки соответствующих структурных частей оформляют крупным шрифтом на отдельной строке.

В тексте не принято делать ссылки на первое лицо, но если необходимо, следует употреблять выражение в третьем лице (например, «автор полагает», «по нашему мнению» и т. п.). Цитаты должны иметь точные ссылки на источники.

Большие таблицы, иллюстрации и распечатки с ЭВМ допускается выполнять в виде приложений. Объем приложений не ограничивается. Страницы текста нумеруются по центру в верхней части листа без каких-либо знаков.

Сокращения слов в тексте не допускаются, кроме установленных ГОСТ 2.316, ГОСТ Р 21.1101, ГОСТ 7.12. Условные буквенные и графические обозначения должны соответствовать установленным стандартам (ГОСТ 2.105).

Обозначения единиц физических величин необходимо принимать в соответствии с ГОСТ 8.417, СН 528.

Переносы слов в заголовках не допускаются. Если заголовок состоит из двух предложений, их разделяют точкой. Расстояние между заголовком и текстом должно быть 15 мм, а между заголовками раздела и подраздела – 8 мм.

Формулы, содержащиеся в отчете, располагают на отдельных строках, нумерация сквозная, арабскими цифрами, которые записывают на уровне формулы справа в круглых скобках. Непосредственно под формулой приводится расшифровка символов и числовых коэффициентов, если они не были пояснены ранее в тексте. Первая строка расшифровки начинается словом «где», которое на-

бирается без абзаца, без двоеточия после него. Выше и ниже каждой формулы должно быть оставлено не менее одной свободной строки. Перечень расшифровки формулы располагают колонкой, символ отделяют от его расшифровки знаком тире. Буквенные обозначения располагаются строго в той же последовательности, в которой они приведены в формуле.

Графики, рисунки, диаграммы и другие иллюстративные материалы помещают в тексте работы по ходу изложения темы или в конце, отдельными приложениями. Каждая иллюстрация должна иметь порядковый номер, обозначаемый цифрами, и тематическое название. Нумерация сквозная по всему отчету.

Приложения оформляются как продолжение работы на последующих страницах, располагать их следует в порядке появления ссылок на них. Каждое приложение должно начинаться с новой страницы и иметь тематический заголовок, написанный прописными буквами.

Отчет по практике составляется и оформляется в период прохождения практики и должен быть закончен к моменту ее окончания. Отчет проверяется руководителем практики. По результатам защиты выставляется дифференцированный зачет.

3. ЗАЩИТА ОТЧЕТА ПО ПРАКТИКЕ

3.1. Порядок защиты

К защите отчета по учебной практике «Учебная практика – ознакомительная практика – Первая учебная практика» допускаются студенты, выполнившие программу практики и представившие в установленные сроки подготовленные материалы.

Защита отчета носит публичный характер и проводится в форме собеседования по темам и разделам практики. Собеседование позволяет выявить уровень знаний обучающегося по проблематике учебной практики, степень самостоятельности студента в выполнении задания. При защите отчета студент освещает цель и задачи работы, раскрывает сущность выполненной работы, отмечает перспективы работы над данной темой и пути внедрения результатов работы в практическую деятельность

При оценивании проделанной работы принимаются во внимание посещаемость практики, качество представленного отчета, защиты отчета и ответов на вопросы.

По результатам аттестации выставляется дифференцированный зачет – «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Оценки «отлично», «хорошо», «удовлетворительно» означают успешное прохождение практики.

3.2. Типовые контрольные вопросы

1. Комплексный подход к обеспечению информационной безопасности, предполагающий рациональное сочетание технологии и средств информационной защиты.
2. Источники, риски и формы атак на информацию.
3. Алгоритмы криптографических преобразований данных для обеспечения целостности, подлинности и конфиденциальности информации.
4. Политика безопасности.
5. Стандарты безопасности.
6. Основные понятия и классификация средств криптографической защиты информации.
7. Криптографические модели.
8. Аппаратно-программные средства защиты информации: средства обеспечения конфиденциальности данных; средства идентификации и аутентификации пользователей; средства аутентификации электронных данных и средства управления ключевой информацией.
9. Модели безопасности основных ОС.
10. Алгоритмы шифрования.
11. Основные свойства симметричных криптосистем.
12. Классическая сеть Фейстеля.
13. Блочные алгоритмы шифрования данных.
14. Алгоритм шифрования DES и AES.
15. Шифрование в режимах CBC, CFB и OFB.
16. Требования к системам защиты информации.
17. Основные свойства асимметричных криптосистем.

18. Однонаправленные функции.
19. Алгоритм шифрования RSA.
20. Криптосистема Эль Гамаля.
21. Криптосистема на основе эллиптических кривых в циклических полях Галуа.
22. Основные свойства хэш-функций. Функция хеширования SHA, MD4, MD5.
23. Функция хеширования ГОСТ Р 34.11-94.
24. Однонаправленные хэш-функции на основе симметричных блочных алгоритмов.
25. Основные свойства цифровой подписи.
26. Алгоритм цифровой подписи RSA. Алгоритм цифровой подписи Эль Гамаля.
27. Отечественный стандарт цифровой подписи на эллиптических кривых (ГОСТР34.10-2001).
28. Алгоритмы аутентификации пользователей.
29. Аутентификация на основе одноразовых и многоразовых паролей.
30. Биометрическая идентификация и аутентификация пользователя.
31. Аутентификация, основанная на симметричных и асимметричных алгоритмах.
32. Генерация и хранение ключей. Распределение ключей. Алгоритм формирования общего секретного ключа.
33. Защита информации в сетях. Концепция построения защищённых виртуальных частных сетей VPN. Функции и компоненты сети VPN. VPN решения для построения защищённых корпоративных сетей.
34. Многоуровневая защита корпоративных сетей.
35. Общие вопросы информационной безопасности в ЛВС.
36. Защита информации при межсетевом взаимодействии.
37. Криптографические протоколы, используемые для защиты технологии клиент-сервер.

3.3. Пример типового контрольного задания
Исследование алгоритма шифрования RSA

I. Цель работы

Цель работы – исследовать математические и прикладные аспекты шифрования данных по алгоритму RSA.

II. Краткая справка об алгоритме RSA

В зависимости от структуры используемых ключей методы шифрования подразделяются на два основных вида:

1) *Симметричное шифрование*: посторонним лицам может быть известен алгоритм шифрования, но неизвестна небольшая порция секретной информации – ключа, одинакового для отправителя и получателя сообщения. Примеры: DES, 3DES, AES, Blowfish, Twofish, ГОСТ 28147-89.

2) *Асимметричное шифрование*: посторонним лицам может быть известен алгоритм шифрования и открытый ключ, но неизвестен закрытый ключ, известный только получателю. Криптографические системы с открытым ключом в настоящее время широко применяются в различных сетевых протоколах, в частности, в протоколах TLS и его предшественнике SSL (лежащих в основе HTTPS), а также SSH, PGP, S/MIME и т. д. Российский стандарт, использующий асимметричное шифрование ГОСТ Р 34.10-2001.

На данный момент асимметричное шифрование на основе открытого ключа RSA (расшифровывается, как Rivest, Shamir and Aldeman – это фамилии создателей алгоритма) использует большинство продуктов на рынке информационной безопасности.

Хотя RSA может теоретически использоваться для шифрования и дешифрования любых реальных сообщений, на практике его наиболее часто применяют для относительно коротких сообщений. В частности, он применяется в цифровых подписях и других криптографических системах, которые нужны для шифрования коротких сообщений без доступа к симметричному ключу.

Криптостойкость RSA основывается на сложности разложения на множители больших чисел, а именно – на исключительной трудности задачи определить секретный ключ на основании откры-

того, так как для этого потребуется решить задачу о существовании делителей целого числа. Наиболее криптостойкие системы используют 1024-битовые и большие ключи.

Примечание: В 2003 г. Ади Шамир и Эран Тромер разработали (на теоретическом уровне) схему специализированного TWIRL-компьютера для взлома RSA-ключей. По их оценке вариант TWIRL-компьютера стоимостью в 10 000 $ позволит дешифровать 512-битовый ключ за 10 минут, а в варианте стоимостью в 10 000 000 $ – 1024-битовый ключ примерно за год. В настоящее время нет сведений об эффективном взломе 1024-битовых ключей. Тем не менее, лаборатория RSA рекомендует в настоящее время использовать ключи размером 2048 бит.

III. Алгоритм шифрования данных по схеме RSA

Шаг 1. Генерация ключей

1. Выбираются два больших простых числа p и q (числа p и q называются порождающими числами).

Примечание: Простое число – целое положительное число, большее единицы, и не имеющее других делителей, кроме самого себя и единицы.

2. Вычисляется произведение порождающих чисел $N = p \times q$ (число N называется модулем).

3. Вычисляется функция Эйлера: $\varphi(N)=(p-1)(q-1)$.

Примечания:

1. Результат расчета данной функции равен количеству положительных чисел, не превосходящих N и взаимно простых с N.

2. Взаимно простые числа – целые числа, не имеющие общих делителей кроме 1. Например, 14 и 25 взаимно простые числа, так как у них нет общих делителей, кроме 1, т.е. НОД (14, 25) = 1 (НОД – наибольший общий делитель).

3. Порождающие числа p и q в дальнейшем не нужны, поэтому они уничтожаются безопасным образом.

4. Выбирается открытый ключ $\boldsymbol{e}$, который должен удовлетворять следующим условиям:

$$1 < \boldsymbol{e} < \varphi(N), \qquad (1)$$

НОД($\boldsymbol{e}$, φ(N)) = 1, т.е. $\boldsymbol{e}$ и φ(N) – взаимно простые числа.

5. Определяется секретный ключ $\boldsymbol{d}$, исходя из выполнения условий (2):

$$\begin{aligned} &\boldsymbol{d} < N, \\ &(\boldsymbol{e} \times \boldsymbol{d}) \bmod \varphi(N) = 1. \end{aligned} \qquad (2)$$

Примечание: mod – деление с остатком. Например: 11 mod 3 = 2 (проверка: 11 = 3 × 2 + 2); 128 mod 33 = 29 (проверка: 128 = 33 × 3 + 29); 7 mod 90 = 7 (проверка: 7 = 90 × 0 + 7).

6. Пара (N, $\boldsymbol{e}$) объявляется открытым ключом абонента и публикуется открыто в общедоступном сертифицированном справочнике, где исключается возможность его подмены (рис. 1).

Абонент	Открытый ключ
A	(N_A, $\boldsymbol{e_A}$)
B	(N_B, $\boldsymbol{e_B}$)
C	(N_C, $\boldsymbol{e_C}$)

Рис. 1

Ключ $\boldsymbol{d}$ является секретным ключом абонента и держится им в секрете.

Примечание: Выбор $\boldsymbol{e}$ в качестве открытого ключа, а $\boldsymbol{d}$ – в качестве секретного, является совершенно условным. Оба ключа совершенно равноправны. В качестве открытого ключа можно взять $\boldsymbol{d}$, а в качестве закрытого – $\boldsymbol{e}$. Главное – закрытый ключ хранить в тайне.

Шаг 2. Шифрование сообщения (действия на стороне отправителя)

7. Исходное сообщение разбивается на блоки, каждый из которых может быть представлен в виде десятичного числа M_i. При этом должно выполняться условие (3):

$$M_i < N. \quad (3)$$

Примечание: Следует отметить, что порождающие числа p и q выбираются таким образом, чтобы N было больше кода любого символа открытого сообщения. В автоматизированных системах исходное сообщение переводиться в двоичное представление, после чего шифрование выполняется над блоками бит, равной длины. При этом длина блока должна быть меньше, чем длина двоичного представления N.

8. Текст открытого (исходного) сообщения шифруется открытым ключом получателя по формуле (4):

$$C_i = M_i^e \bmod N, \quad (4)$$

где C_i – i-й символ шифрограммы, представленный в десятичном коде; M_i – i-й символ исходного сообщения, представленный в десятичном коде.

Зашифрованное сообщение (шифрограмма) отправляется получателю.

Шаг 3. Расшифровка шифрограммы (действия на стороне получателя)

9. Принятая шифрограмма расшифровывается с использованием секретного ключа получателя по формуле (5):

$$M_i = C_i^d \bmod N. \quad (5)$$

IV. Порядок выполнения задания

Постановка задачи:

Два абонента, Олег и Сергей, передают друг другу данные с использованием алгоритма шифрования RSA. Смоделируйте:

а) передачу сообщения *ПРИВЕТ_СЕРГЕЙ* от Олега → Сергею.

б) расшифровку полученного сообщения на стороне Сергея.

Коды букв соответствуют их положению в русском алфавите. Для символа (_) используется код 0.

Для генерации открытого и секретного ключей Сергей использует порождающие числа $p = 3$ и $q = 11$.

1. Откройте файл **Исследование RSA.xlsx**. В таблицу **Генерация ключей** занесите значения p и q Сергея. Введите формулы для вычисления N и $\varphi(N)$.

Генерация ключей		
	Олег	Сергей
p		3
q		11
N		33
$\varphi(N)$		20

Рис. 2

2. Случайным образом выберите открытый ключ ***e***, при этом проверьте выполнение условий (1).

Для подбора ключа ***e*** вводите с клавиатуры в ячейку **J10** целые числа и проверяйте значение в ячейке **J14** (в эту ячейку введена функция **НОД**, вычисляющая наибольший общий делитель для ячеек **J9** и **J10**). Если **J14 = 1**, то введенное в ячейку **J10** число подходит в качестве открытого ключа ***e***. Условиям (1) удовлетворяют числа: 3, 7, 9, 11, 13, 17, 19.

Для возможности последующего выполнения в Excel операций возведения чисел в большие степени выберите в качестве открытого ключа ***e*** наименьшее из возможных чисел, т.е. число 3**.**

Генерация ключей		
	Олег	Сергей
p		3
q		11
N		33
$\varphi(N)$		20
e		3
d		
Проверка подбора ключей		
e		1

Рис. 3

3. Подберите вручную значение секретного ключа ***d***, чтобы выполнялись условия (2).

Для этого в ячейку **J15** введите функцию **ОСТАТ** (категория **Математические**), которая реализует операцию **mod** (остаток от деления). После этого начните вводить с клавиатуры в ячейку **J11** целые числа и проверяйте значение в ячейке **J15**. Если **J15 = 1**, то введенное в ячейку **J11** число подходит в качестве секретного ключа ***d*** (рис. 4).

$\varphi(N)$		20
e		3
d		7
Проверка подбора ключей		
e		1
d		1

Рис. 4

4. Используя формулу (4) зашифруйте коды символов открытым ключом Сергея (рис. 5).

Символы и их шифрограммы					
№ п/п	Символ	Код символа	Шифрограмма символа (откр. ключ Олега)	Шифрограмма символа (откр. ключ Сергея)	Символ
1	А	1		1	А
2	Б	2		8	Б
3	В	3		27	В
4	Г	4		31	Г
5	Д	5		26	Д
6	Е	6		18	Е

Рис. 5

5. Используя функцию **ВПР** (категория **Ссылки и массивы**), составьте шифрограмму сообщения *ПРИВЕТ_СЕРГЕЙ* (рис. 6).

Примечание: Функцию **ВПР** используйте в режиме точного поиска, т.е. аргумент *Интервальный_просмотр* = 0. Напомним, что функция **ВПР** ищет значение в крайнем левом столбце таблицы и возвращает значение ячейки, находящейся в указанном столбце той же строки (так как аргумент *Интервальный_просмотр* = 0, то сортировку таблицы производить не надо). При возникновении затруднений воспользуйтесь справочной системой по данной функции.

Шифрограмма сообщения от Олега ---> Сергею								
Открытое сообщение	П	Р	И	В	Е	Т	_	С
Шифрограмма сообщения	4	29	3	27	18	28	0	24

Рис. 6

6. Используя формулу (5), расшифруйте шифрограмму, полученную от Олега (рис. 7).

Расшифровка полученной шифрограммы Сергеем								
Шифрограмма сообщения	4	29	3	27	18	28	0	24
Расшифрованная шифрограмма	16	17	9	3	6	19	0	18

Рис. 7

7. Используя функцию **ВПР**, составьте исходное сообщение, отправленное Олегом (рис. 8).

Расшифровка полученной шифрограммы Сергеем								
Шифрограмма сообщения	4	29	3	27	18	28	0	24
Расшифрованная шифрограмма	16	17	9	3	6	19	0	18
Сообщение	П	Р	И	В	Е	Т	_	С

Рис. 8

8. Создайте копию листа **Основы RSA**. Переименуйте лист **Основы RSA (2)** в **Расширение RSA**.

9. Допустим, что для кодирования символов используется кодовая таблица Windows-1251. Закодируйте все символы, представленные в таблице **Символы и шифрограмм**ы, в соответствии с данной кодировкой. Для этого воспользуйтесь функцией **КОДСИМВ** (категория **Текстовые**), рис. 9.

Символы и их шифрограммы				
№ п/п	Символ	Код символа	Шифрограмма символа (откр. ключ Олега)	Ш (откр
1	А	192		
2	Б	193		
3	В	194		
4	Г	195		
5	Д	196		

Рис. 9

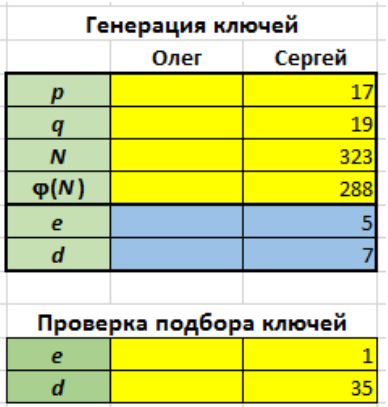
Обратите внимание, что исходное сообщение не может быть составлено, так как расшифровка шифрограммы происходит некорректно из-за нарушения условия (3).

Расшифровка полученной шифрограммы Сергеем								
Шифрограмма сообщения	3	10	8	2	32	12	2	11
Расшифрованная шифрограмма	9	10	2	29	32	12	29	11
Сообщение	#Н/Д	#Н/Д	#Н/Д	#Н/Д	#Н/Д	#Н/Д	#Н/Д	#Н/Д

Рис. 10

10. Выберите новые порождающие числа $p = 17$ и $q = 19$. Обратите внимание, что вычисленное значение $N = p \times q = 17 \times 19 = 323 > M_i$.

Выберите открытый ключ ***e***, при этом проверьте выполнение условий (1). Условиям (1) удовлетворяют числа: 5, 7, 11, 13, 17 и т.д. Для возможности последующего выполнения в Excel операций возведения чисел в большие степени выберите в качестве открытого ключа ***e*** наименьшее из возможных чисел, т.е. число 5 (рис. 11).



Генерация ключей		
	Олег	Сергей
p		17
q		19
N		323
φ(*N*)		288
e		5
d		7

Проверка подбора ключей		
e		1
d		35

Рис. 11

11. Подобрать вручную секретный ключ ***d*** для рассматриваемой ситуации является достаточно затруднительной операцией, поэтому воспользуйтесь следующей формулой:

$$\boldsymbol{d} = \boldsymbol{e}^{(\varphi(N)-1)} \bmod \varphi(N). \qquad (6)$$

Введите формулу (6) в ячейку **J11** – обратите внимание, что она возвращает значение ошибки #ЧИСЛО! (рис. 12). Причиной этого является невозможность нахождения в Excel точного значения выражения $\boldsymbol{e}^{(\varphi(N)-1)} = \boldsymbol{e}^{(288-1)} = \boldsymbol{e}^{287}$ с использованием стандартного оператора возведения в степень.

φ(N)		288
e		5
d		#ЧИСЛО!

Проверка подбора ключей		
e		1
d		#ЧИСЛО!

Рис. 12

Вычислите выражение e^{287} mod 288 с использованием программы **Калькулятор** (вид **Инженерный**), входящей в группу стандартных программ Windows. Удалите из ячейки **J11** введенную формулу и занесите в неё вычисленное значение ***d***.

Проверьте правильность подбора вычисленного секретного ключа ***d*** по значению в ячейке **J11** (рис. 13).

φ(N)		288
e		5
d		173

Проверка подбора ключей		
e		1
d		1

Рис. 13

12. В качестве передаваемого сообщения от Олега → Сергею введите слово *СЕТЬ*. Незадействованные ячейки очистите (рис. 14)

Шифрограмма сообщения от Олега ---> Сергею						
Открытое сообщение	С	Е	Т	Ь		
Шифрограмма сообщения	133	125	58	254		

Рис. 14

13. Обратите внимание, что при дешифровке полученной шифрограммы с использованием функции **ОСТАТ** возвращается значение ошибки #ЧИСЛО! (рис. 15).

Расшифровка полученной шифрограммы Сергеем						
Шифрограмма сообщения	133	125	58	254		
Расшифрованная шифрограмма	#ЧИСЛО!	#ЧИСЛО!	#ЧИСЛО!	#ЧИСЛО!		
Сообщение	#ЧИСЛО!	#ЧИСЛО!	#ЧИСЛО!	#ЧИСЛО!		

Рис. 15

Дешифруйте полученную шифрограмму, используя программу **Калькулятор**. Удалите из ячеек функцию **ОСТАТ** и занесите в них дешифрованные коды символов. При правильной дешифровке будет сформировано слово *СЕТЬ* (рис. 16).

Расшифровка полученной шифрограммы Сергеем (с использованием программы Калькулятор)								
Шифрограмма сообщения	133	125	58	254				
Расшифрованная шифрограмма	209	197	210	220				
Сообщение	С	Е	Т	Ь				

Рис. 16

14. Смоделируйте передачу сообщения *ТЕКСТ_ПОЛУЧИЛ* от Сергея → Олегу, если для генерации открытого и секретного ключей Олег использует порождающие числа $p = 59$ и $q = 73$.

В таблицу **Генерация ключей** занесите значения p и q Олега. Определите N и $\varphi(N)$, рис. 17.

Генерация ключей		
	Олег	Сергей
p	59	17
q	73	19
N	4307	323
$\varphi(N)$	4176	288
e		5
d		173

Рис. 17

15. Допустим, Олег выбрал открытый ключ ***e*** = 737. В ячейку **I14** скопируйте из ячейки **J14** функцию **НОД**, проверьте выполнение условия (1), рис. 18.

φ(*N*)	4176	288
e	737	5
d		173
Проверка подбора ключей		
e	1	1
d		1

Рис. 18

В ячейку **I15** скопируйте из ячейки **J15** функцию **ОСТАТ**.

Используя программу **Калькулятор** вычислите значение секретного ключа ***d*** по формуле (6).

Обратите внимание на сообщение программы **Калькулятор** (рис. 19), поясните причину возникновения данного сообщения.

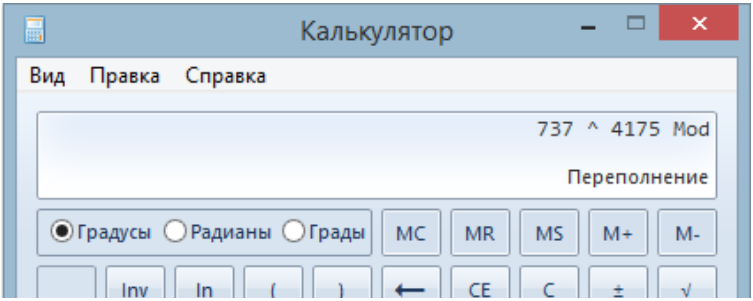


Рис. 19

16. Как можно было убедиться, выражение 737^{4175} не может быть вычислено программой **Калькулятор**. Следует заметить, что большинство компьютерных языков и прикладных программ не имеет операторов, которые могут эффективно вычислять степень для очень больших чисел. Чтобы можно было выполнять данную

операцию, используют специальные алгоритмы. Для рассматриваемой ситуации интерес представляют алгоритмы, способные вычислить выражение

$$y = a^x \bmod m \qquad (7)$$

при больших x. Такие алгоритмы получили название *алгоритмов быстрого возведения в степень по модулю*. Наиболее известными из них являются: метод с использованием Китайской теоремы об остатках, метод возведения в квадрат и умножения, метод Монтгомери возведения в степень, алгоритм с использованием «школьного» метода.

Рассмотрим *метод возведения в квадрат и умножения* с использованием схемы «справа налево», который можно достаточно просто реализовать в MS Excel. Рассмотрение метода проведем на конкретном примере вычисления секретного ключа Олега с использованием выражения

$$737^{4175} \bmod 4176.$$

а) Подготовьте таблицу для ввода исходных данных (рис. 20).

Вычисление секретного ключа Олега методом возведения в квадрат и умножения (схема «справа налево»)		
Число (*a*)	737	<--- *e* - открытый ключ Олега
Степень (*x*)	4175	<--- φ(N)-1
Модуль (*m*)	4176	<--- φ(N)

Рис. 20

б) Показатель степени $x = 4175$ представьте в двоичной системе счисления и запишите полученное значение в обратном порядке с выделением разрядов (рис. 21). Необходимые для этого действия рассмотрены под рисунком.

Модуль (*m*)	4176	<--- φ(N)					
Степень дв.	1000001001111						
Число разрядов	13						
Номер разряда	13	12	11	10	9	8	7
Степ. дв. обр. Текст	1	1	1	1	0	0	1
Степ дв. обр. Число	1	1	1	1	0	0	1

Рис. 21

Для представления числа в двоичной системе счисления воспользуйтесь функцией **ОСНОВАНИЕ** из категории **Математические** (функция доступна в версиях Excel 2013 и более поздних) или программой **Калькулятор** (вид **Программист**).

Примечание: В ранних версиях Excel в категории **Инженерные** имеется функция **ДЕС.В.ДВ**, которая выполняет преобразование чисел из диапазона от -512 до 511, что для рассматриваемого примера является недостаточным. Функция **ОСНОВАНИЕ** выполняет преобразование чисел от 0 до 2^{53}.

Для подсчета числа разрядов двоичного числа воспользуйтесь функцией **ДЛСТР** (категория **Текстовые**).

Номера разрядов двоичного числа введите вручную, начиная с 13 и до 1 (для последующего выделения разрядов в обратном порядке).

Для выделения разрядов из двоичного числа воспользуйтесь функцией **ПСТР** (категория **Текстовые**). Результатом будет поразрядное представление двоичного числа в обратном порядке (1111001000001), поэтому рассматриваемая схема и называется «справа налево».

Так как функция **ПСТР** возвращает текстовые значения, то для последующих расчетов их необходимо преобразовать в числовые. Для этого воспользуйтесь функцией **ЗНАЧЕН** (категория **Текстовые**).

в) Разработайте расчетную таблицу (рис. 22). Необходимые для этого действия рассмотрены под рисунком.

Степ. дв. обр. текст	1	1	1	1
Степ дв. обр. Число	1	1	1	1

№ п/п	Степень. дв. обр.	y_i	
1	1	737	<--- 737 mod 4176
2	1	289	<--- 737^2 mod 4176
3	1	1	<--- 289^2 mod 4176
4	1	1	<--- 1^2 mod 4176
5	0	1	<--- 1^2 mod 4176
6	0	1	<--- 1^2 mod 4176
7	1	1	<--- 1^2 mod 4176
8	0	1	<--- 1^2 mod 4176
9	0	1	<--- 1^2 mod 4176
10	0	1	<--- 1^2 mod 4176
11	0	1	<--- 1^2 mod 4176
12	0	1	<--- 1^2 mod 4176
13	1	1	<--- 1^2 mod 4176
	Произведение *Y*	212993	
	Секр. ключ *d*	17	

Рис. 22

В столбце **Степень. дв. обр.** приведено двоичное представление степени x в обратном порядке (вверху младшие разряды, внизу – старшие), для чего необходимо транспонировать (развернуть на 90 градусов) значения из строки **Степ дв. обр**. Для этого воспользуйтесь функцией **ТРАНСП** (категория **Ссылки и массивы**), которая должна быть введена как формула массива. Порядок действий следующий:

- введите функцию **ТРАНСП** в первую ячейку столбца **Степень. дв. обр.**;
- выделите все ячейки столбца **ТРАНСП**, поставьте курсор в строку формул;
- нажмите комбинацию клавиш **Ctrl+Shift+Enter**.

Первое значение в столбце y_i рассчитывается по формуле:

$$y_1 = e \bmod \varphi(N) = 737 \bmod 4176 = 737.$$

Дальнейшие вычисления производятся по рекуррентной формуле:

$$y_i = (y_{i-1})^2 \bmod \varphi(N). \qquad (8)$$

Введите соответствующие формулы в столбец $\boldsymbol{y_i}$.

Для нахождения итогового произведения Y необходимо перемножить y_i, которым соответствует 1 в двоичном представлении степени (столбец **Степень. дв. обр.**). Для рассматриваемого примера имеем:

$$Y = y_1 \times y_2 \times y_3 \times y_4 \times y_7 \times y_{13}.$$

Для автоматизации данного расчета введите в ячейку **Произведение *Y*** следующую формулу:

=ПРОИЗВЕД(ЕСЛИ(*Диапазон_двоичных_разрядов*=1; *Диапазон_y_i*;1)).

Данная формула должна быть введена как формула массива, т.е. с использованием комбинации клавиш **Ctrl+Shift+Enter**.

Примечание: Суть формулы состоит в том, что если разряд в двоичном представлении степени равен 1, то в итоговое произведение Y в качестве сомножителя будет входить y_i, в противном случае в качестве сомножителя будет входить 1. Для рассматриваемого примера имеем: $Y = y_1 \times y_2 \times y_3 \times y_4 \times 1 \times 1 \times y_7 \times 1 \times 1 \times 1 \times 1 \times 1 \times y_{13}$.

Секретный ключ $\boldsymbol{d}$ рассчитывается по формуле:

$$\boldsymbol{d} = Y \bmod \varphi(N).$$

17. В рассматриваемом примере легко подобрать такие порождающие числа p и q, что при расчете $\boldsymbol{d}$ даже с использованием рассмотренного выше метода возникает переполнение и возвращается значение ошибки #ЧИСЛО. Кроме того, операцию возведения в

большие степени необходимо будет повторить достаточно большое число раз при кодировании символов открытым ключом Олега и при дешифровке полученной шифрограммы на стороне Сергея. Поэтому возникает потребность в написании специальной функции на языке VBA, которая позволит решать данную задачу более эффективно

В рамках выполняемой работы не предполагается изучение VBA, поэтому такая функция уже подготовлена, её необходимо импортировать в программный модуль проекта и использовать на рабочем листе Excel.

Для возможности использования функций, написанных на языке VBA, необходимо сохранить рабочую книгу с поддержкой макросов (**Сохранить как – Книга Excel с поддержкой макросов (*.xlsm)**).

Для импорта функции выполните следующие действия:

- перейдите в среду VBA (вкладка **Разработчик – Visual Basic** или комбинация кнопок **Alt+F11**);
- вставьте программный модуль (**Insert – Module**);
- импортируйте функцию **СтепеньПоМодулю** из файла **Функция СтепеньПоМодулю 32.bas** (**Insert – File**). При импорте выберите тип файла **Basic Files (*.bas)** или **All Files (*.*)**.

Если Вы используется 64-разрядную версию MS Office то можно импортировать функцию **СтепеньПоМодулю** из файла **Функция СтепеньПоМодулю 64.bas**, в которой для переменных используется тип данных **LongLong**, позволяющий хранить 8-байтовые целые числа в диапазоне от -9 223 372 036 854 775 808 до 9 223 372 036 854 775 807 (в 32-разрядной версии функции используется тип данных **Long**, позволяющий хранить 4-байтовые целые числа в диапазоне от -2 147 483 648 до 2 147 483 647);

- нажмите кнопку **Save**, закройте окно VBA и перейдите на рабочий лист.

18. Протестируйте импортированную функцию **СтепеньПоМодулю** (категория **Определенные пользователем**), вычислив с её помощью секретный ключ ***d*** (рис. 23).

1	1	<--- 1^2 mod 4176
Произведение *Y*	**212993**	
Секр. ключ *d*	**17**	
Секр. ключ *d* (VBA)	**17**	

Рис. 23

19. Используйте функцию **СтепеньПоМодулю** для кодирования символов открытым ключом Олега (рис. 24).

№ п/п	Символ	Код символа	Шифрограмма символа (откр. ключ Олега)
1	А	192	3331
2	Б	193	1520
3	В	194	695
4	Г	195	873
5	Д	196	711
6	Е	197	1730
7	Ж	198	2671
8	З	199	1528

Рис. 24

20. Путем копирования создайте шаблон для шифрования сообщения *ТЕКСТ_ПОЛУЧИЛ*, передаваемого от Сергея → Олегу, и шаблон для расшифровки полученной шифрограммы на стороне Олега (рис. 25).

Шифрограмма сообщения от Сергея ---> Олегу											
Открытое сообщение	Т	Е	К	С	Т	_	П	О	Л	У	
Шифрограмма сообщения											
Расшифровка полученной шифрограммы Олегом (с использованием функции СтепеньПоМодулю)											
Шифрограмма сообщения											
Расшифрованная шифрограмма											
Сообщение											

Рис. 25

21. Используя функцию **ВПР**, составьте шифрограмму сообщения *ТЕКСТ_ПОЛУЧИЛ* (рис. 26).

Шифрограмма сообщения от Сергея ---> Олегу								
Открытое сообщение	Т	Е	К	С	Т	_	П	О
Шифрограмма сообщения	592	1730	737	3713	592	241	505	2091

Рис. 26

22. Используя функцию **СтепеньПоМодулю**, расшифруйте шифрограмму, полученную от Сергея (рис. 27).

Примечание: В качестве второго аргумента функции **СтепеньПоМодулю** используйте значение секретного ключа ***d***.

Расшифровка полученной шифрограммы Олегом (с использованием функции СтепеньПоМодулю)								
Шифрограмма сообщения	592	1730	737	3713	592	241	505	2091
Расшифрованная шифрограмма	210	197	202	209	210	95	207	206

Рис. 27

23. Используя функцию **ВПР**, составьте исходное сообщение, отправленное Сергеем (рис. 28).

Расшифровка полученной шифрограммы Олегом (с использованием функции СтепеньПоМодулю)								
Шифрограмма сообщения	592	1730	737	3713	592	241	505	2091
Расшифрованная шифрограмма	210	197	202	209	210	95	207	206
Сообщение	Т	Е	К	С	Т	_	П	О

Рис. 28

24. Таким образом в ходе проделанной работы были изучены математические и прикладные аспекты шифрования данных по алгоритму RSA, который получил широкое распространение в различных сетевых протоколах, а также в электронной цифровой подписи.

Криптостойкость RSA основывается на сложности разложения на множители больших чисел, а именно – на исключительной трудности задачи определить секретный ключ на основании открытого, так как для этого потребуется решить задачу о существовании делителей целого числа.

В рассмотренном примере использовались 6-битовое ($p = 59$) и 7-битовое ($q = 73$) порождающие числа для формирования ключей, тем не менее даже при такой малой размерности в ряде случаев

пришлось прибегнуть к нестандартным вычислениям. В реальных системах используются, как правило, 1024-битовые ключи, а наиболее криптостойкие системы используют 2048-битовые ключи.

3.4. Шкала и критерии оценивания

Оценка			
«2» (неудовлетворительно)	**Пороговый уровень освоения**	**Углубленный уровень освоения**	**Продвинутый уровень освоения**
	«3» (удовлетворительно)	**«4» (хорошо)**	**«5» (отлично)**
Практика не пройдена или студент не предоставил отчет по практике. Не владеет необходимыми теоретическими знаниями по направлению планируемой работы. Необходимые практические компетенции не сформированы.	Практика пройдена. При защите отчета по практике студент демонстрирует слабую теоретическую подготовку. Собранные материалы представляют минимальный объем необходимой информации.	Практика пройдена. При защите отчета студент демонстрирует хорошую теоретическую подготовку. Собранные материалы представлены в объеме, достаточном для составления отчета, дана хорошая оценка собранной информации.	Практика пройдена. При защите отчета студент демонстрирует высокую теоретическую подготовку. Представленные материалы содержат всю информацию, необходимую для составления отчета. Защищаемый отчет выполнен на высоком уровне.
Регулярность посещения занятий практики - менее 50 % занятий практики	Регулярность посещения занятий практики - не менее 50 % занятий практики	Регулярность посещения занятий практики – не менее 70 % занятий практики	Регулярность посещения занятий практики - не менее 85 % занятий практики

4. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕОБЕСПЕЧЕНИЕ

4.1. Основная литература

1. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - 5-е изд., перераб. и доп. - М.: Форум: НИЦ ИНФРА-М, 2014. - 432 с.: ил.; 60x90 1/16. - (Профессиональное образование). (http://znanium.com/catalog/product/420047)

2. *Гвоздева, В.А.* Информатика, автоматизированные информационные технологии и системы [Электронный ресурс]: учебник / В.А. Гвоздева. – М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2015. – 544. (http://znanium.com/catalog.php?bookinfo=492670)

3. *Царев, Р.Ю.* Программные и аппаратные средства информатики [Электронный ресурс]: учебник / Р.Ю. Царев, А.В. Прокопенко, А.Н. Князьков; Министерство образования и науки Российской Федерации, Сибирский Федеральный университет. – Красноярск: Сибирский федеральный университет, 2015. – 160 с. (http://biblioclub.ru/index.php?page=book_red&id=435670)

4.2. Дополнительная литература

1. *Кияев, В.И.* Развитие информационных технологий [Электронный ресурс] / В.И. Кияев, О.Н. Граничин. – 2-е изд., исправ. – М.: Национальный Открытый Университет «ИНТУИТ», 2016. – 199 с. (http://biblioclub.ru/index.php?page=book_red&id=428804)

2. *Гагарина, Л.Г.* Современные проблемы информатики и вычислительной техники [Электронный ресурс]: учебное пособие / Л.Г. Гагарина, А.А. Петров. – М.: ИД ФОРУМ: ИНФРА-М, 2011. – 368 с. (http://znanium.com/catalog.php?bookinfo=203313)

3. *Федосеев, С.В.* Современные проблемы прикладной информатики [Электронный ресурс]: хрестоматия / С.В. Федосеев. – М.: Евразийский открытый институт, 2011. – 271 с. (http://biblioclub.ru/index.php?page=book_red&id=93186)

4. *Губарев, В.В.* Информатика: прошлое, настоящее, будущее [Электронный ресурс]: учебное пособие / В.В. Губарев. – М.: РИЦ "Техносфера", 2011. – 432 с. (http://biblioclub.ru/index.php?page=book_red&id=135404)

4.3. Базы данных и электронно-библиотечные системы

1. Европейская цифровая библиотека Europeana: http://www.europeana.eu/portal
2. КонсультантПлюс: справочно-поисковая система [Электронный ресурс]. – www.consultant.ru/
3. Информационно-издательский центр по геологии и недропользованию Министерства природных ресурсов и экологии Российской Федерации - ООО "ГЕОИНФОРММАРК": http://www.geoinform.ru/
4. Информационно-аналитический центр «Минерал»: http://www.mineral.ru/
5. Мировая цифровая библиотека: http://wdl.org/ru
6. Научная электронная библиотека «Scopus»: https://www.scopus.com
7. Научная электронная библиотека ScienceDirect: http://www.sciencedirect.com
8. Научная электронная библиотека «eLIBRARY»: https://elibrary.ru/
9. Портал «Гуманитарное образование» http://www.humanities.edu.ru/
10. Федеральный портал «Российское образование» http://www.edu.ru/
11. Федеральное хранилище «Единая коллекция цифровых образовательных ресурсов» http://school-collection.edu.ru/
12. Поисковые системы Yandex, Rambler, Yahoo и др.
13. Электронно-библиотечная система издательского центра «Лань»: https://e.lanbook.com/books
14. Электронная библиотека Российской Государственной Библиотеки (РГБ): http://elibrary.rsl.ru/
15. Электронная библиотека учебников: http://studentam.net
16. Электронно-библиотечная система «ЭБС ЮРАЙТ»: www.biblio-online.ru.
17. Электронная библиотечная система «Национальный цифровой ресурс «Руконт»»: http://rucont.ru/
18. Электронно-библиотечная система http://www.sciteclibrary.ru/

Приложение 1

БЛАНК ЗАДАНИЯ НА ПРАКТИКУ

ПЕРВОЕ ВЫСШЕЕ ТЕХНИЧЕСКОЕ УЧЕБНОЕ ЗАВЕДЕНИЕ РОССИИ

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего профессионального образования

САНКТ-ПЕТЕРБУРГСКИЙ ГОРНЫЙ УНИВЕРСИТЕТ

ЗАДАНИЕ НА ПРАКТИКУ

Студент (ФИО)_____шифр_____

Вид практики_____

Место проведения практики_____

Срок проведения практики_____

Руководитель практики_____

1. Тема _____

2. Содержание практики_____

_____

_____

3. План практики

№ п.п.	Вид работы	Срок выполнения	Отметка о выполнении

Руководитель практики _____ _____
(подпись, дата) (инициалы, фамилия)

Студент _____ _____
(подпись, дата) (инициалы, фамилия)

Приложение 2

ТИТУЛЬНЫЙ ЛИСТ ОТЧЕТА ПО ПРАКТИКЕ

ПЕРВОЕ ВЫСШЕЕ ТЕХНИЧЕСКОЕ УЧЕБНОЕ ЗАВЕДЕНИЕ РОССИИ

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования

САНКТ-ПЕТЕРБУРГСКИЙ ГОРНЫЙ УНИВЕРСИТЕТ

ОТЧЕТ ПО ПРАКТИКЕ

Студента (ФИО) _____, шифр_____

Вид практики _____

Место прохождения практики _____

Сроки прохождения практики _____

Руководитель практики _____

1. Тема _____

_____

_____

2. Содержание практики (вид работы, срок выполнения) _____

_____

_____

_____

_____

Студент _____ _____

(подпись, дата) (инициалы, фамилия)

3. Заключение руководителя _____

_____

_____

4. Руководитель практики _____ _____

(подпись, дата) (инициалы, фамилия)

СОДЕРЖАНИЕ