

Министерство образования Пензенской области
Государственное автономное профессиональное образовательное учреждение
Пензенской области
«Пензенский колледж информационных и промышленных технологий
(ИТ-колледж)»

УТВЕРЖДАЮ

Зам. директора по ООП
Е.А. Волобуева

«30» августа 2022 г.

**РАБОЧАЯ ПРОГРАММА
ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ
«ЗАНИМАТЕЛЬНОЕ ШИФРОВАНИЕ»**

Формы организации: кружок по криптографии.

Программа предназначена для работы со студентами первого курса (16-17 лет).

Срок реализации программы – 1 год.

Разработчик: преподаватель ГАПОУ ПО «ПКИПТ»
Хмелевская Елена Борисовна

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Программа курса внеурочной деятельности «Занимательное шифрование» составлена на основе следующих нормативных документов:

- Федеральный государственный образовательный стандарт основного общего образования;
- ОПОП СПО по специальности 11.02.12 Почтовая связь.

Актуальность курса состоит в том, что он направлен на расширение знаний учащихся по математике, информатике, развитие их теоретического мышления и логической культуры. Криптография одно из перспективных направлений в науке по практической значимости.

Программа позволяет преподавателю комплексно решать образовательные задачи, а учащимся ознакомиться со многими интересными вопросами математики, информатики, выходящими за рамки школьной программы и программы СПО. Решение задач по криптографии закрепит интерес обучающихся к познавательной деятельности, будет способствовать развитию мыслительных операций и общему интеллектуальному развитию. С целью повышения познавательной активности обучающихся, формирования способности самостоятельного освоения материала студенты имеют возможность познакомиться с научно – популярной литературой по проблеме применения математики. Предполагается использование компьютеров в практической части курса.

Цели курса:

- формирование представления о комбинаторике и теории вероятности;
- обучение: основным понятиям криптографии, основным способам шифрования и дешифрования текста, строгой математической проверки стойкости шифра;
- развитие навыков построения математических моделей шифров, алгоритмизации, программирования, навыков анализа своей деятельности;
- развитие логического мышления;
- воспитание усидчивости, внимания.

Задачи курса:

- изучить основы комбинаторики и теории вероятности;
- расширить кругозор в области фундаментальных наук, показать их практическую значимость;
- сформировать навыки элементарного построения криптосистем;

- изучить основные способы шифрования и дешифрования текста;
- сформировать чёткое понимание стойкости шифра;
- научить проверять стойкость шифра математическими расчётами;
- развить навыки программирования;
- научить создавать программный продукт на основе различных основных математических, криптографических систем;
- реализовать технические и эвристические способности учащихся в ходе проектирования и программирования различных криптографических задач;
- развить навык анализа выполненной работы;
- рассмотреть применение полученных навыков в различных областях знаний;
- развить у учащихся логическое мышление;
- воспитать у учащихся усидчивость и внимание.

Настоящая программа рассчитана на 1 год обучения и предназначена для работы со студентами первого курса (16-17 лет). Занятия проводятся 1 раз в неделю по 1 часу (34 часа в год).

Формы организации учебных занятий: индивидуальная, групповая, работа в парах с последующим коллективным обсуждением результатов, урок-игра, урок-беседа, проектный урок, игры на внимание, смотр знаний, мини-лекция, урок-турнир.

От уровня подготовленности и состава группы зависит объем теоретического материала и перечень тем для занятий. Тематика занятий отражает реальные познавательные интересы студентов, содержит полезную и любопытную информацию, интересные математические факты, способные дать простор воображению.

Список информационных источников

Литература для преподавателя

1. А.В. Бабаш, Г.П. Шанкин «Криптография» Москва, СОЛОН-Р, 2019 г.
2. С.И. Бобровский «Delphi 7. Учебный курс» Санкт-Петербург, Питер, 2018г.
3. Ростовцев А.Г., Маховенко Е.Б. Теоретическая криптография. – М.: Изд. Професионал, 2019.
4. Алферов А.П., Зубков А.К., Кузьмин А.С., Черемушкин А.В. Основы криптографии: Учебное пособие. – М.: Гелиос АРВ, 2017.
5. <http://mathinfinity.net.ru/article/6/> различные шифры
6. <http://www.rbardalzo.narod.ru/kripto2.html> криптография и математика

Для студента

1. Адаменко, Михаил Основы классической криптологии. Секреты шифров и кодов / Михаил Адаменко. - Москва: Машиностроение, 2018. - 256 с
2. Бабаш, А. В. История криптографии. Часть I / А.В. Бабаш, Г.П. Шанкин. - М.: Гелиос АРВ, 2018.
3. Баричев С. Криптография без секретов. – 2016.
4. Криптография: скоростные шифры / А. Молдовян и др. - М.: БХВ-Петербург, 2017. - 496 с.

http://wiki.saripkro.ru/index.php/Исследование_учащихся_Секреты_криптографии

ПРОГРАММА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ

Планируемые результаты курса «Занимательное шифрование»

Личностные результаты

У обучающегося будут сформированы:

- умение ясно, точно, грамотно излагать свои мысли в устной и письменной речи, понимать смысл поставленной задачи, выстраивать аргументацию, приводить примеры и контрпримеры;
- критичность мышления, умение распознавать логически некорректные высказывания, отличать гипотезу от факта;
- креативность мышления, инициатива, находчивость, активность при решении задач по криптографии;
- способность к эмоциональному восприятию математических объектов, задач, решений, рассуждений;

Обучающийся получит возможность для формирования:

- широких познавательных интересов, инициативы и любознательности, мотивов познания и творчества;
- готовности и способности к саморазвитию и реализации творческого за счет развития их образного, алгоритмического и логического мышления;
- интереса к математике, информатике стремления использовать полученные знания в процессе обучения другим предметам и в жизни;
- чувства личной ответственности за качество окружающей информационной среды.

Метапредметные результаты освоения курса

У обучающегося будут сформированы:

- умение находить в различных источниках информацию, необходимую для решения математических проблем, представлять ее в понятной форме, принимать решение в условиях неполной и избыточной, точной и вероятностной информации;
- умение понимать и использовать математические средства наглядности (графики, диаграммы, таблицы, схемы и др.) для иллюстрации, интерпретации, аргументации;
- умение выдвигать гипотезы при решении учебных задач, понимать необходимость их проверки;
- умение применять индуктивные и дедуктивные способы рассуждений, видеть различные стратегии решения задач;

- умение самостоятельно ставить цели, выбирать и создавать алгоритмы для решения учебных проблем;

- умение планировать и осуществлять деятельность, направленную на решение задач исследовательского характера;

- создание моделей криптографических систем;

- оценивание стойкости созданного шифра.

Обучающийся получит возможность для формирования умений:

- владение основными универсальными умениями математического характера: постановка и формулирование проблемы; поиск и выделение необходимой информации, применение методов информационного поиска; структурирование и визуализация информации; выбор наиболее эффективных способов решения задач в зависимости от конкретных условий;

- использования средств информационных и коммуникационных технологий для сбора, хранения, преобразования и передачи различных видов информации, навыки создания личного информационного пространства.

Предметные результаты освоения курса

У обучающегося будут сформированы:

- умения работать с текстом (структурирование, извлечение необходимой информации), точно и грамотно выражать свои мысли в устной и письменной речи, применяя математическую терминологию и символику, использовать различные языки математики (словесный, символический, графический), развития способности обосновывать суждения, проводить классификацию;

- умения пользоваться изученными математическими формулами;

- знания основных способов представления и анализа статистических данных; умения решать задачи с помощью перебора всех возможных вариантов;

- умения решать простые комбинаторные задачи;

- умения работать с текстовыми файлами;

- умения применять изученные понятия, результаты и методы при решении задач из различных разделов курса, в том числе задач, не сводящихся к непосредственному применению известных алгоритмов.

ТЕМАТИЧЕСКИЙ ПЛАН

№	Разделы	Количество часов
I	Введение в криптографию и первые шифры	4
II	Математические основы криптографии	9
III	Современные криптосистемы	10
IV	Решение задач	11
	Итого	34

СОДЕРЖАНИЕ ПРОГРАММЫ ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ «СЕКРЕТЫ КРИПТОГРАФИИ»

Раздел	Теоретическая часть	Практическая часть
Введение в криптографию и первые шифры	Инструктаж по технике безопасности. Как защитить свое послание. Из истории криптографии. Где применяется и как применяется. Поиск информации по теме «Способы шифрования» (работа в парах)	Обзорная лекция с элементами практической работы. Поиск сценарий применения полученных знаний в жизни. Мозговой штурм.
Математические основы криптографии	Мини-лекции: – Основы криптоанализа. Криптостойкость. – Криптоатака. – Подстановка. – Шифр Цезаря. – Перестановка.	Игры на внимание. Практическое занятие. Использование ПО «Практические задания по криптографии»
Современные криптосистемы	Гаммирование. Основные понятия теории вероятности. Блочные шифры. Современные криптосистемы с открытым ключом. Для чего компьютеру нужна криптография? Как зашифровать файл? Современные средства криптозащиты. Электронная цифровая подпись. Алгоритм Диффи-Хеллмана. Криптография и криптовалюта. Что такое «блокчейн»?	Практикум по решению задач. Игры. Урок –турнир «Шерлок Холмс». Использование ПО «Практические задания по криптографии»

Решение задач	Блиц-опрос по пройденному материалу	Решение учащимися готовых задач, составление задач по теме. Выставка работ, на которых представлен зашифрованный текст. Проектный урок. Урок- турнир. Смотр знаний «Математическое лото». Конкурс на лучшую презентацию
---------------	-------------------------------------	---

Введение в криптографию и первые шифры

Студент научится:

- оперировать на базовом уровне понятиями: шифр, криптография, стеганография, Скитала, диск и линейка Энея; цифровая тайнопись.
- извлекать, интерпретировать и преобразовывать информацию о криптографии.

Математические основы криптографии

Студент научится:

- оперировать на базовом уровне понятиями: выборка, перестановка, подстановка, делимость чисел, НОД;
- изменять действия для шифрования и дешифрования;
- создавать шифр на основе перестановки.
- извлекать, интерпретировать и преобразовывать информацию о шифре.

Современные криптосистемы

Студент научится:

- оперировать на базовом уровне понятиями: криптосистемы с секретным ключом; метод гаммирования; псевдослучайные числа; криптосистема, криптоанализ.
- оперировать современными методами шифрования;
- создавать шифры на основе блочных.

Решение задач

Студент научится:

- решать несложные задачи на шифрование и дешифрование;
- строить модель условия задачи (в виде таблицы, схемы, рисунка);

- осуществлять способ поиска решения задачи, в котором рассуждение строится от условия к требованию или от требования к условию;

- составлять план решения задачи;
- выделять этапы решения задачи;
- моделировать рассуждения при поиске решения задач с помощью граф-схемы;
- интерпретировать результаты в задаче, исследовать полученное решение задачи;
- решать и конструировать задачи на основе рассмотрения реальных ситуаций, в которых не требуется точный результат.

Контроль за усвоением изучаемого материала осуществляется по итогам защиты проектов.

Примерные темы проектов:

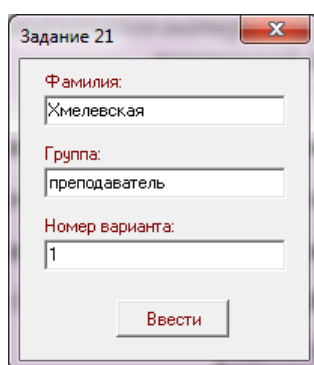
1. Секреты криптографии
 2. Криптография – основа информационной безопасности
 3. Как защитить свою информацию
 4. Современные криптосистемы
- и т.д.

МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПРОГРАММЫ ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ «СЕКРЕТЫ КРИПТОГРАФИИ»

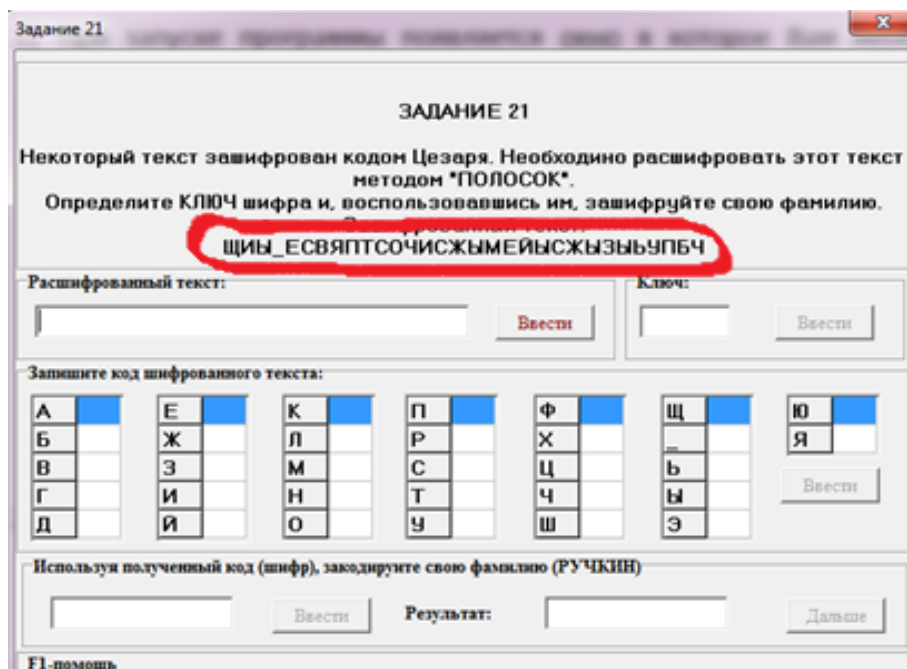
**Образец контрольно-оценочного материала, разработанного в ходе реализации программы
внеурочной деятельности*

Инструкция по использованию программы с задачей по криптографии.

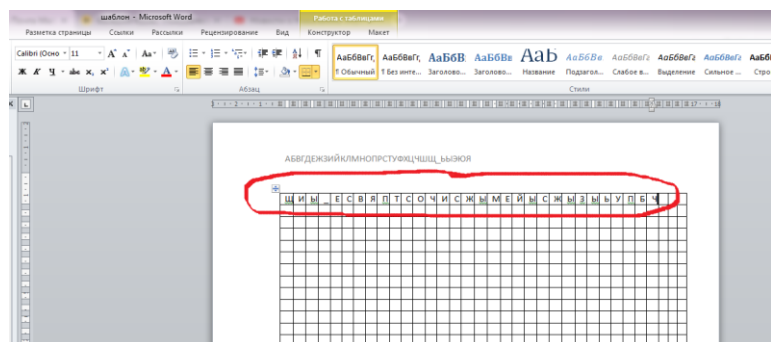
- 1) При запуске программы появится окно, в которое Вам необходимо ввести:
поле 1 – фамилию русскими буквами,
поле 2 – номер группы (введенная информация значения не имеет),
поле 3 – номер варианта (выбираете разные варианты, начиная с «1»).



- 2) После ввода регистрационных данных, открывается само задание. В нем указано зашифрованное сообщение, которое и нужно расшифровать, используя метод «Полосок». Для удобства расшифровки воспользуйтесь файлом «шаблон.docx».



- 3) В верхнюю строку этого документа Вы переписываете зашифрованное сообщение, начиная с верхней левой ячейки, по одному символу, слева – направо.

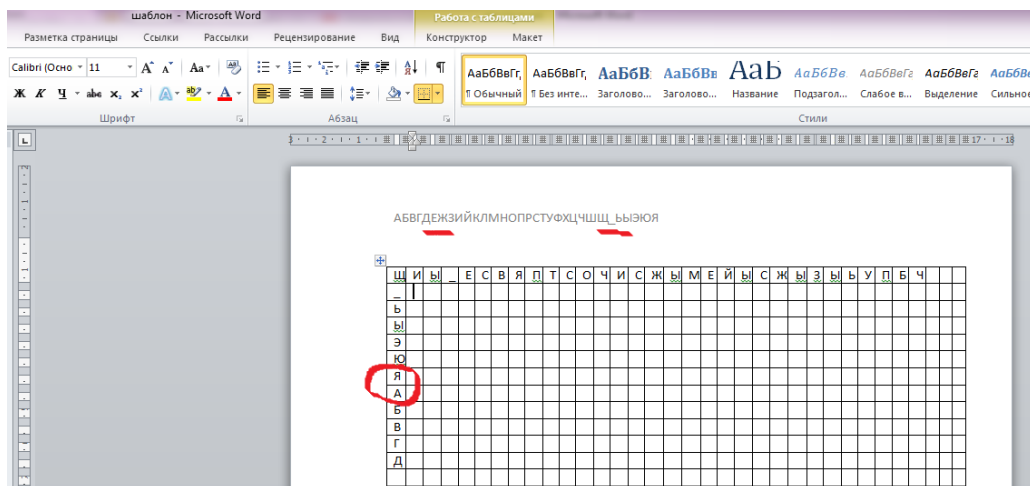


- 4) Далее, используя подсказку над таблицей, Вы заполняете каждый столбец указанным порядком символов не менее чем на 12 строк вниз.

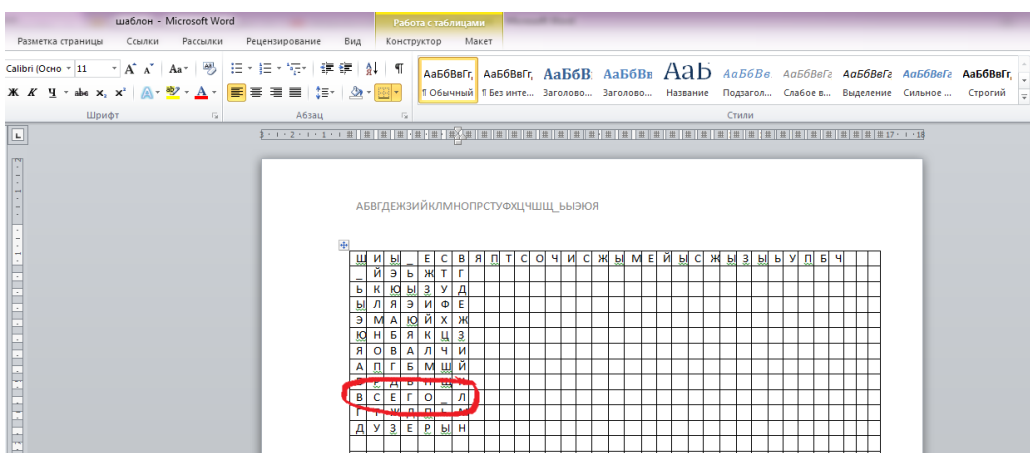
Внимание!

А) обратите внимание на отсутствие в порядке символов букв «ё» и «ъ», однако, имеется символ «_».

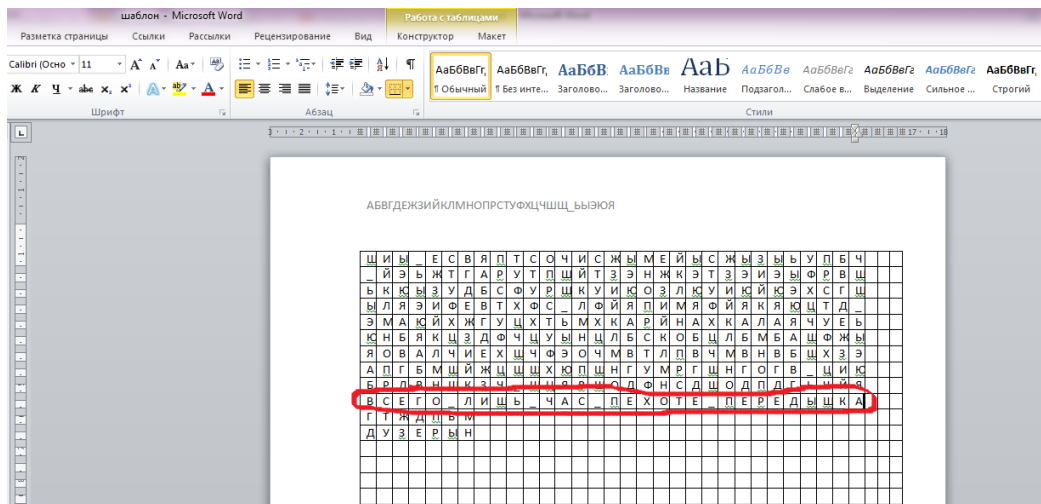
Б) При заполнении столбцов, дойдя до буквы «я», Вы не останавливаетесь, а продолжаете заполнять буквами «а», «б»....



- 5) На этапе заполнения очередного столбца в одной из строк Вам представится известное слово или его часть. В этой-то строке и окажется расшифрованное Вами сообщение.



- 6) Заполните все столбцы до той строки, в которой «обнаружилась» часть расшифрованного сообщения.



7) Введите расшифрованное сообщение в интерфейс программы и нажмите «Ввести».

Задание 21

ЗАДАНИЕ 21

Некоторый текст зашифрован кодом Цезаря. Необходимо расшифровать этот текст методом "ПОЛОСОК".

Определите КЛЮЧ шифра и, воспользовавшись им, зашифруйте свою фамилию.

Зашифрованный текст:
ЩИЫ_ЕСВЯПТТСОЧИСЖЫМЕЙЫСЖЫЗЫЬУПБЧ

Расшифрованный текст:
ЕГО_ЛИШЬ_ЧАС_ПЕХОТЕ_ПЕРЕДЫШКА

Ключ:

Запишите код шифрованного текста:

А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я

Используя полученный код (шифр), закодируйте свою фамилию (РУЧКИН)

Результат:

F1-помощь

8) В случае правильности ввода, станет активным окно для ввода ключа, в противном – появится ошибка.

9) В поле «Ключ:» введите значение:

если вариант 1 – «23»,

вариант 2 – «24»,

вариант 3 – «25»

и т. д. и нажмите «Ввести».

Задание 21

ЗАДАНИЕ 21

Некоторый текст зашифрован кодом Цезаря. Необходимо расшифровать этот текст методом "ПОЛОСОК".

Определите КЛЮЧ шифра и, воспользовавшись им, зашифруйте свою фамилию.

Зашифрованный текст:
ЩИЫ_ЕСВЯПТСОЧИСЖЫМЕЙЫСЖЫЗЫЬУПБЧ

Расшифрованный текст:

Ключ:

Запишите код шифрованного текста:

А	Ч	Е	Ы	К	Б	П	Ж	Ф	Л	Щ	Р	Ю	Х
Б	Ш	Ж	Э	Л	В	Р	З	Х	М	С	Т	Я	Ц
В	Щ	З	Ю	М	Г	С	И	Ц	Н	Ь	У		
Г		И	Я	Н	Д	Т	Й	Ч	О	Ы	У		
Д	Ь	Й	А	О	Е	У	К	Ш	П	Э	Ф		

Используя полученный код (шифр), закодируйте свою фамилию (РУЧКИН)

Результат:

F1-помощь

- 11) Активным становится поле для ввода Вашей фамилии в зашифрованном виде. Используйте для этого ранее заполненный код, т. е. каждую букву фамилии Вы записываете как она представлена в зашифрованном виде. Нажимаете «Ввести».

Задание 21

ЗАДАНИЕ 21

Некоторый текст зашифрован кодом Цезаря. Необходимо расшифровать этот текст методом "ПОЛОСОК".

Определите КЛЮЧ шифра и, воспользовавшись им, зашифруйте свою фамилию.

Зашифрованный текст:
ЩИЫ_ЕСВЯПТСОЧИСЖЫМЕЙЫСЖЫЗЫЬУПБЧ

Расшифрованный текст:

Ключ:

Запишите код шифрованного текста:

А	Ч	Е	Ы	К	Б	П	Ж	Ф	Л	Щ	Р	Ю	Х
Б	Ш	Ж	Э	Л	В	Р	З	Х	М	С	Т	Я	Ц
В	Щ	З	Ю	М	Г	С	И	Ц	Н	Ь	У		
Г		И	Я	Н	Д	Т	Й	Ч	О	Ы	У		
Д	Ь	Й	А	О	Е	У	К	Ш	П	Э	Ф		

Используя полученный код (шифр), закодируйте свою фамилию (РУЧКИН)

Результат:

F1-помощь

В результате вы должны увидеть свою фамилию в ее расшифрованном виде. На этом задание можно считать выполненным. Рекомендуется выполнить это задание в нескольких вариантах.

ОБРАЗЕЦ РЕШЕНИЯ

АБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩ_ЬЫЭЮЯ

[illegible]

ШАБЛОН ДЛЯ РЕШЕНИЯ

[illegible]