МИНОБРНАУКИ РОССИИ

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ**

**УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**

Лабораторная работа

Криптографические методы защиты информации.  
Шифрование методом простой (однозначной) замены.

|  |  |  |
| --- | --- | --- |
| Преподаватель | \_\_\_\_\_\_ | С. Ю. Сидельникова |
| Обучающийся | \_\_\_\_\_\_ | В. В. Павук |

Воронеж 2021

**Зашифрованный текст**

ВКДЖЮТОДЧЮЫБМДЩХШЮДЖКФЭЫЧЮХШЭКУДКШФЫГТОБЮЕМШДЫШЯФОТЭОЕДЩХШЮШРБЩУОАДЩХШЮДЖКФЭЫЧЮЦШДЫЯФЮЭОФШЯЫФКБЮШЯКБМГКСЫЕОБОЮШДОШКЕДКРЮЕРЦШВШКЯФОТОБОДДКЮШЯФОТЭОЕДКЮШКАБЫРЕЮШСШЮДЖКФЭЫЧЮКДДКЮШРЮРЕОЭОШКДЫШЮЪФЫОЕШЕОЗДЮЬОРВЩХШФКБМШДКШООШФЫРВФИЕЮОШКРКАОДДКШКЯЫРДКШЯКРВКБМВЩШКДКШЬФОСЫЕКШЯКБЩЬОДЮОЭШДОРЫДВЧЮКДЮФКСЫДДКЪКШТКРЕЩЯЫШВКШСРОЮШЮДЖКФЭЫЧЮЮШСШЕКЭШЬЮРБОШЯФОТЭОЕДКЮШТЫУОШОРБЮШЮДЖКФЭЫЧЮЦШЗФЫДЮЕРЦШСШВКЭЯМХЕОФОШЮБЮШЯФОТДЫГДЫЬОДЫШТБЦШВКЭЯМХЕОФДКЪКШЮРЯКБМГКСЫДЮЦШЩЪФКГИШООШВКДЖЮТОДЧЮЫБМДКРЕЮШЭКЪЩЕШДКРЮЕМШДОВКЭЯМХЕОФДИЮШЮШСККАЙОШДОЕОЗДЮЬОРВЮЮШЗЫФЫВЕОФШЭДКЪЮЭШБХТЦЭШЯФЮЗКТЮЕРЦШСИРЕЩЯЫЕМШСШВЫЬОРЕСОШЯКБМГКСЫЕОБОЮШДОШКТДКЮШЫШЧОБКЪКШФЦТЫШРЮРЕОЭШЮДЖКФЭЫЧЮКДДИЗШРОФСЮРКСШОРБЮШТБЦШТКРЕЩЯЫШВШЕЫВЮЭШРЮРЕОЭЫЭШЮРЯКБМГЩХЕРЦШЭДКЪКФЫГКСИОШЯЫФКБЮШЮБЮШЮДЫЦШВКДЖЮТОДЧЮЫБМДЫЦШЮДЖКФЭЫЧЮЦШЕКШДЫСОФДЦВЫШЛЕЮШТЫДДИОШАЩТЩЕШЗФЫДЮЕМРЦШДОШЕКБМВКШСШЪКБКСОШДКШЮШСШГЫЯЮРДКЮШВДЮУВОШЮБЮШДЫШБЮРЕВЫЗШАЩЭЫЪЮШВКЕКФИОШЯКБМГКСЫЕОБМШЬЫРЕКШКРЕЫСБЦОЕШДЫШФЫАКЬОЭШРЕКБОШЫШЕКШЮШЯКЯФКРЕЩШЕОФЦОЕШЮШТОБКШГТОРМШДОШСШДОКФЪЫДЮГКСЫДДКРЕЮШБХТОЮШЫШСШЮГДЫЬЫБМДКЮШДОЯФЮЪКТДКРЕЮШЯЫФКБМДКЮШРЗОЭИШДОСКГЭКУДКШЯКЭДЮЕМШЭДКЪКШФЫГДИЗШЯЫФКБОЮШФОВКЭОДТЫЧЮЮШЯКШЮЗШФОЪЩБЦФДКЮШЯКШСКГЭКУДКРЕЮШЬЫРЕКЮШРЭОДОШЕКБМВКШЩРЩЪЩАБЦХЕШЯКБКУОДЮОШГЫРЕЫСБЦЦШЯФЮЭОДЦЕМШДОРБКУДИОШРЗОЭИШЬОФОТКСЫДЮЦШЮБЮШСККАЙОШРЕЫФЫЕМРЦШРСОРЕЮШТОБКШВШТСЩЭШЕФОЭШБОЪВКШГЫЯКЭЮДЫОЭИЭШЮШРЕКБМШУОШБОЪВКШЩЪЫТИСЫОЭИЭШЯЫФКБЦЭШКЯЮРЫДДИЮШВБЫРРШЩЦГСЮЭИЗШЭОРЕШЭКУДКШДЫГСЫЕМШФЫГЭОЙОДЮОЭШВКДЖЮТОДЧЮЫБМДИЗШТЫДДИЗШСШРФОТОШЪТОШЮЭШДОШКАОРЯОЬОДЫШГЫЬЫРЕЩХШЮШДОШЭКУОЕШАИЕМШДОКАЗКТЮЭЫЦШГЫЙЮЕЫШЩЪФКГЫШУОШРКРЕКЮЕШСШЕКЭШЬЕКШЭДКЪЮОШДОШКЕВЫУЩЕРЦШЩГДЫЕМШРОВФОЕИШВКЕКФИОШРЫЭЮШЯФКРЦЕРЦШСШФЩВЮШЯКЭЮЭКШЯЫФКБОЮШЗФЫДЦЙЮЗРЦШСШГЫЯЮРДИЗШВДЮУВЫЗШЯКБМГКСЫЕОБОЮШСШЛЕКЕШВБЫРРШЯКЯЫТЫОЕШЯОФОТЫЬЫШВКДЖЮТОДЧЮЫБМДИЗШТЫДДИЗШСШКЕВФИЕКЭШСЮТОШСШФЫГЪКСКФОШСШЯЮРМЭОШЯКШРОЕЮШВКЕКФЫЦШТОБЫОЕШСКГЭКУДИЭШЯОФОЗСЫЕШТЫДДИЗШТБЦШЫЕЫВЮШЭКЪЩЕШЮРЯКБМГКСЫЕМРЦШФЫГДИОШЕОЗДЮЬОРВЮОШРФОТРЕСЫШЯКТРБЩНЮСЫДЮОШЮБЮШЯФКРБЩНЮСЫДЮОШФЫГЪКСКФКСШЯЫРРЮСДКОШЯФКРБЩНЮСЫДЮОШРОЕЮШДКШЮТОЦШКТДЫШКРЩЙОРЕСЮЕМШТКРЕЩЯШВШТЫДДИЭШСШЕКЕШЭКЭОДЕШВКЪТЫШКДЮШДЫЮЭОДООШГЫЙЮЙОДИШРБЩУОАДЫЦШЮДЖКФЭЫЧЮЦШДЫЯФЮЭОФШЯЫФКБЮШЯКБМГКСЫЕОБОЮШДОШКЕДКРЮЕРЦШВШКЯФОТОБОДДКЮШЯФОТЭОЕДКЮШКАБЫРЕЮШСШЮДЖКФЭЫЧЮКДДКЮШРЮРЕОЭОШКДЫШЮЪФЫОЕШЕОЗДЮЬОРВЩХШФКБМ

**Статистика каждой буквы**

[('П', 0.0), (' ', 0.0), ('Л', 0.001), ('Н', 0.001), ('А', 0.007), ('Ж', 0.007), ('Х', 0.007), ('У', 0.008), ('Ч', 0.008), ('Ь', 0.009), ('З', 0.012), ('Ъ', 0.012), ('И', 0.015), ('Г', 0.016), ('Щ', 0.018), ('М', 0.019), ('Ц', 0.019), ('В', 0.022), ('Т', 0.024), ('С', 0.029), ('Я', 0.029), ('Б', 0.035), ('Э', 0.035), ('Ф', 0.04), ('Р', 0.047), ('Е', 0.052), ('Ы', 0.065), ('Д', 0.072), ('Ю', 0.078), ('О', 0.081), ('К', 0.094), ('Ш', 0.135)]

**Ключ:**

Дальше я сопоставляю два алфавита по их частоте. Из частотного анализа текста мы получаем, что Ш, скорее всего кодирует пробел. Получился следующий текст

ПОАЮИДЕАЧИТЛЯАЫЖ ИАЮОРВТЧИЖ ВОХАО РТЗДЕЛИНЯ АТ КРЕДВЕНАЫЖ И СЛЫХЕШАЫЖ ИАЮОРВТЧИУ АТКРИВЕР КТРОЛИ КОЛЯЗОМТНЕЛЕИ АЕ ОНАОСИНСУ П ОКРЕДЕЛЕААОИ КРЕДВЕНАОИ ОШЛТСНИ М ИАЮОРВТЧИОААОИ СИСНЕВЕ ОАТ ИЬРТЕН НЕБАИГЕСПЫЖ РОЛЯ АО ЕЕ РТСПРЪНИЕ ОСОШЕААО

ОКТСАО КОСПОЛЯПЫ ОАО ГРЕМТНО КОЛЫГЕАИЕВ АЕСТАПЧИОАИРОМТААОЬО ДОСНЫКТ ПО МСЕИ ИАЮОРВТЧИИ М НОВ ГИСЛЕ КРЕДВЕНАОИ ДТХЕ ЕСЛИ ИАЮОРВТЧИУ БРТАИНСУ М ПОВКЯЖНЕРЕ ИЛИ КРЕДАТЗАТГЕАТ ДЛУ ПОВКЯЖНЕРАОЬО ИСКОЛЯЗОМТАИУ ЫЬРОЗЪ ЕЕ ПОАЮИДЕАЧИТЛЯАОСНИ ВОЬЫН АОСИНЯ АЕПОВКЯЖНЕРАЪИ И МООШЕ АЕНЕБАИГЕСПИИ БТРТПНЕР ВАОЬИВ ЛЖДУВ КРИБОДИНСУ МЪСНЫКТНЯ М ПТГЕСНМЕ КОЛЯЗОМТНЕЛЕИ АЕ ОДАОИ Т ЧЕЛОЬО РУДТ СИСНЕВ ИАЮОРВТЧИОААЪБ СЕРМИСОМ ЕСЛИ ДЛУ ДОСНЫКТ П НТПИВ СИСНЕВТВ ИСКОЛЯЗЫЖНСУ ВАОЬОРТЗОМЪЕ КТРОЛИ

ИЛИ ИАТУ ПОАЮИДЕАЧИТЛЯАТУ ИАЮОРВТЧИУ НО АТМЕРАУПТ ЭНИ ДТААЪЕ ШЫДЫН БРТАИНЯСУ АЕ НОЛЯПО М ЬОЛОМЕ АО И М ЗТКИСАОИ ПАИХПЕ ИЛИ АТ ЛИСНПТБ ШЫВТЬИ ПОНОРЪЕ КОЛЯЗОМТНЕЛЯ ГТСНО ОСНТМЛУЕН АТ РТШОГЕВ СНОЛЕ Т НО И КОКРОСНЫ НЕРУЕН И ДЕЛО ЗДЕСЯ АЕ М

АЕОРЬТАИЗОМТААОСНИ ЛЖДЕИ Т М ИЗАТГТЛЯАОИ АЕКРИЬОДАОСНИ КТРОЛЯАОИ СБЕВЪ АЕМОЗВОХАО КОВАИНЯ ВАОЬО РТЗАЪБ КТРОЛЕИ РЕПОВЕАДТЧИИ КО ИБ РЕЬЫЛУРАОИ КО МОЗВОХАОСНИ ГТСНОИ СВЕАЕ НОЛЯПО ЫСЫЬЫШЛУЖН КОЛОХЕАИЕ ЗТСНТМЛУУ КРИВЕАУНЯ АЕСЛОХАЪЕ СБЕВЪ ГЕРЕДОМТАИУ ИЛИ МООШЕ СНТРТНЯСУ СМЕСНИ ДЕЛО П ДМЫВ НРЕВ ЛЕЬПО ЗТКОВИАТЕВЪВ И СНОЛЯ ХЕ ЛЕЬПО ЫЬТДЪМТЕВЪВ КТРОЛУВ ОКИСТААЪИ ПЛТСС ЫУЗМИВЪБ ВЕСН ВОХАО АТЗМТНЯ РТЗВЕЕАИЕВ ПОАЮИДЕАЧИТЛЯАЪБ ДТААЪБ М СРЕДЕ ЬДЕ ИВ АЕ ОШЕСКЕГЕАТ ЗТГТСНЫЖ И АЕ ВОХЕН ШЪНЯ АЕОШБОДИВТУ ЗТИНТ ЫЬРОЗТ ХЕ СОСНОИН М НОВ ГНО ВАОЬИЕ АЕ ОНПТХЫНСУ ЫЗАТНЯ СЕПРЕНЪ ПОНОРЪЕ СТВИ КРОСУНСУ М РЫПИ КОВИВО КТРОЛЕИ БРТАУИБСУ М ЗТКИСАЪБ ПАИХПТБ КОЛЯЗОМТНЕЛЕИ М ЭНОН ПЛТСС КОКТДТЕН КЕРЕДТГТ ПОАЮИДЕАЧИТЛЯАЪБ ДТААЪБ М ОНПРЪНОВ МИДЕ М РТЗЬОМОРЕ М КИСЯВЕ КО СЕНИ ПОНОРТУ ДЕЛТЕН МОЗВОХАЪВ КЕРЕБМТН ДТААЪБ ДЛУ ТНТПИ ВОЬЫН ИСКОЛЯЗОМТНЯСУ РТЗАЪЕ НЕБАИГЕСПИЕ СРЕДСНМТ КОДСЛЫЦИМТАИЕ ИЛИ КРОСЛЫЦИМТАИЕ РТЗЬОМОРОМ КТССИМАОЕ КРОСЛЫЦИМТАИЕ СЕНИ АО ИДЕУ ОДАТ ОСЫЕСНМИНЯ ДОСНЫК П ДТААЪВ М НОН ВОВЕАН ПОЬДТ ОАИ АТИВЕАЕЕ ЗТИЕАЪ СЛЫХЕШАТУ ИАЮОРВТЧИУ АТКРИВЕР КТРОЛИ КОЛЯЗОМТНЕЛЕИ АЕ ОНАОСИНСУ П ОКРЕДЕЛЕААОИ КРЕДВЕНАОИ ОШЛТСНИ М ИАЮОРВТЧИОААОИ СИСНЕВЕ ОАТ ИЬРТЕН НЕБАИГЕСПЫЖ РОЛЯ

Пока что сложно что-то понять. Я начинаю анализировать предлоги, союзы, окончания слов.

В итоге перебора вариантов я получаю следующий ключ

C['Д'] = 'Н'

C['Ы'] = 'А'

C['Л'] = 'О'

C['И'] = 'Ы'

C['Е'] = 'Т'

C['С'] = 'В'

C['З'] = 'Е'

C['У'] = 'Ж'

C['М'] = 'Ь'

C['Э'] = 'М'

C['Х'] = 'Х'

C['Я'] = 'П'

C['Ж'] = 'Ф'

C['Ь'] = 'Ь'

C['В'] = 'К'

C['Ц'] = 'Я'

C['Ч'] = 'Ц'

C['Щ'] = 'У'

C['Х'] = 'Ю'

C['Б'] = 'Л'

C['А'] = 'Б'

C['Ь'] = 'Ч'

C['Ъ'] = 'Г'

C['З'] = 'Х'

C['Н'] = 'Ш'

**Код программы:**

T = {

    'А' : 0,

    'Б' : 0,

    'В' : 0,

    'Г' : 0,

    'Д' : 0,

    'Е' : 0,

    'Ж' : 0,

    'З' : 0,

    'И' : 0,

    'К' : 0,

    'Л' : 0,

    'М' : 0,

    'Н' : 0,

    'О' : 0,

    'П' : 0,

    'Р' : 0,

    'С' : 0,

    'Т' : 0,

    'У' : 0,

    'Ф' : 0,

    'Х' : 0,

    'Ц' : 0,

    'Ч' : 0,

    'Ш' : 0,

    'Щ' : 0,

    'Ь' : 0,

    'Ы' : 0,

    'Ъ' : 0,

    'Э' : 0,

    'Ю' : 0,

    'Я' : 0,

    ' ' : 0,

}

alphabet = {

    'А' : 0.062,

    'Б' : 0.014,

    'В' : 0.038,

    'Г' : 0.013,

    'Д' : 0.025,

    'Е' : 0.072,

    'Ж' : 0.007,

    'З' : 0.016,

    'И' : 0.062,

    'К' : 0.028,

    'Л' : 0.035,

    'М' : 0.026,

    'Н' : 0.053,

    'О' : 0.09,

    'П' : 0.023,

    'Р' : 0.04,

    'С' : 0.045,

    'Т' : 0.053,

    'У' : 0.021,

    'Ф' : 0.002,

    'Х' : 0.009,

    'Ц' : 0.004,

    'Ч' : 0.012,

    'Ш' : 0.006,

    'Щ' : 0.003,

    'Ь' : 0.014,

    'Ы' : 0.016,

    'Ъ' : 0.014,

    'Э' : 0.003,

    'Ю' : 0.006,

    'Я' : 0.018,

    ' ' : 0.13

}

**for** i **in** string:

**for** j **in** T**.keys**():

**if** (j **==** i):

            T[j] = T[j] + 1

**break**

**for** i **in** T**.keys**():

    T[i] = **round**(T[i] / len(string), 3)

alphabetSorted = **sorted**(alphabet**.items**(), key=**lambda** x: x[1])

TSorted = **sorted**(T**.items**(), key=**lambda** x: x[1])

**print**(TSorted)

A = []

B = []

stringNew = ''

**for** i **in** **range**(len(alphabetSorted)):

    A**.append**(alphabetSorted[i][0])

    B**.append**(TSorted[i][0])

C = **dict**(zip(B,A))

C['Д'] = 'Н'

C['Ы'] = 'А'

C['Л'] = 'О'

C['И'] = 'Ы'

C['Е'] = 'Т'

C['С'] = 'В'

C['З'] = 'Е'

C['У'] = 'Ж'

C['М'] = 'Ь'

C['Э'] = 'М'

C['Х'] = 'Х'

C['Я'] = 'П'

C['Ж'] = 'Ф'

C['Ь'] = 'Ь'

C['В'] = 'К'

C['Ц'] = 'Я'

C['Ч'] = 'Ц'

C['Щ'] = 'У'

C['Х'] = 'Ю'

C['Б'] = 'Л'

C['А'] = 'Б'

C['Ь'] = 'Ч'

C['Ъ'] = 'Г'

C['З'] = 'Х'

C['Н'] = 'Ш'

**for** x **in** C**.keys**():

**print**(x, ' - ', C[x])

**for** i **in** string:

**for** j **in** C**.keys**():

**if** i **==** j:

            stringNew += C[j]

**print**(stringNew)

**Дешифрованный текст:**

*КОНФИДЕНЦИАЛЬНУЮ ИНФОРМАЦИЮ МОЖНО РАЗДЕЛИТЬ НА ПРЕДМЕТНУЮ И СЛУЖЕБНУЮ ИНФОРМАЦИЯ НАПРИМЕР ПАРОЛИ ПОЛЬЗОВАТЕЛЕИ НЕ ОТНОСИТСЯ К ОПРЕДЕЛЕННОИ ПРЕДМЕТНОИ ОБЛАСТИ В ИНФОРМАЦИОННОИ СИСТЕМЕ ОНА ИГРАЕТ ТЕХНИЧЕСКУЮ РОЛЬ НО ЕЕ РАСКРЫТИЕ ОСОБЕННО*

*ОПАСНО ПОСКОЛЬКУ ОНО ЧРЕВАТО ПОЛУЧЕНИЕМ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА КО ВСЕИ ИНФОРМАЦИИ В ТОМ ЧИСЛЕ ПРЕДМЕТНОИ ДАЖЕ ЕСЛИ ИНФОРМАЦИЯ ХРАНИТСЯ В КОМПЬЮТЕРЕ ИЛИ ПРЕДНАЗНАЧЕНА ДЛЯ КОМПЬЮТЕРНОГО ИСПОЛЬЗОВАНИЯ УГРОЗЫ ЕЕ КОНФИДЕНЦИАЛЬНОСТИ МОГУТ НОСИТЬ НЕКОМПЬЮТЕРНЫИ И ВООБЕ НЕТЕХНИЧЕСКИИ ХАРАКТЕР МНОГИМ ЛЮДЯМ ПРИХОДИТСЯ ВЫСТУПАТЬ В КАЧЕСТВЕ ПОЛЬЗОВАТЕЛЕИ НЕ ОДНОИ А ЦЕЛОГО РЯДА СИСТЕМ ИНФОРМАЦИОННЫХ СЕРВИСОВ ЕСЛИ ДЛЯ ДОСТУПА К ТАКИМ СИСТЕМАМ ИСПОЛЬЗУЮТСЯ МНОГОРАЗОВЫЕ ПАРОЛИ*

*ИЛИ ИНАЯ КОНФИДЕНЦИАЛЬНАЯ ИНФОРМАЦИЯ ТО НАВЕРНЯКА ОТИ ДАННЫЕ БУДУТ ХРАНИТЬСЯ НЕ ТОЛЬКО В ГОЛОВЕ НО И В ЗАПИСНОИ КНИЖКЕ ИЛИ НА ЛИСТКАХ БУМАГИ КОТОРЫЕ ПОЛЬЗОВАТЕЛЬ ЧАСТО ОСТАВЛЯЕТ НА РАБОЧЕМ СТОЛЕ А ТО И ПОПРОСТУ ТЕРЯЕТ И ДЕЛО ЗДЕСЬ НЕ В*

*НЕОРГАНИЗОВАННОСТИ ЛЮДЕИ А В ИЗНАЧАЛЬНОИ НЕПРИГОДНОСТИ ПАРОЛЬНОИ СХЕМЫ НЕВОЗМОЖНО ПОМНИТЬ МНОГО РАЗНЫХ ПАРОЛЕИ РЕКОМЕНДАЦИИ ПО ИХ РЕГУЛЯРНОИ ПО ВОЗМОЖНОСТИ ЧАСТОИ СМЕНЕ ТОЛЬКО УСУГУБЛЯЮТ ПОЛОЖЕНИЕ ЗАСТАВЛЯЯ ПРИМЕНЯТЬ НЕСЛОЖНЫЕ СХЕМЫ ЧЕРЕДОВАНИЯ ИЛИ ВООБЕ СТАРАТЬСЯ СВЕСТИ ДЕЛО К ДВУМ ТРЕМ ЛЕГКО ЗАПОМИНАЕМЫМ И СТОЛЬ ЖЕ ЛЕГКО УГАДЫВАЕМЫМ ПАРОЛЯМ ОПИСАННЫИ КЛАСС УЯЗВИМЫХ МЕСТ МОЖНО НАЗВАТЬ РАЗМЕЕНИЕМ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ В СРЕДЕ ГДЕ ИМ НЕ ОБЕСПЕЧЕНА ЗАЧАСТУЮ И НЕ МОЖЕТ БЫТЬ НЕОБХОДИМАЯ ЗАИТА УГРОЗА ЖЕ СОСТОИТ В ТОМ ЧТО МНОГИЕ НЕ ОТКАЖУТСЯ УЗНАТЬ СЕКРЕТЫ КОТОРЫЕ САМИ ПРОСЯТСЯ В РУКИ ПОМИМО ПАРОЛЕИ ХРАНЯИХСЯ В ЗАПИСНЫХ КНИЖКАХ ПОЛЬЗОВАТЕЛЕИ В ОТОТ КЛАСС ПОПАДАЕТ ПЕРЕДАЧА КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ В ОТКРЫТОМ ВИДЕ В РАЗГОВОРЕ В ПИСЬМЕ ПО СЕТИ КОТОРАЯ ДЕЛАЕТ ВОЗМОЖНЫМ ПЕРЕХВАТ ДАННЫХ ДЛЯ АТАКИ МОГУТ ИСПОЛЬЗОВАТЬСЯ РАЗНЫЕ ТЕХНИЧЕСКИЕ СРЕДСТВА ПОДСЛУШИВАНИЕ ИЛИ ПРОСЛУШИВАНИЕ РАЗГОВОРОВ ПАССИВНОЕ ПРОСЛУШИВАНИЕ СЕТИ НО ИДЕЯ ОДНА ОСУЕСТВИТЬ ДОСТУП К ДАННЫМ В ТОТ МОМЕНТ КОГДА ОНИ НАИМЕНЕЕ ЗАИЕНЫ СЛУЖЕБНАЯ ИНФОРМАЦИЯ НАПРИМЕР ПАРОЛИ ПОЛЬЗОВАТЕЛЕИ НЕ ОТНОСИТСЯ К ОПРЕДЕЛЕННОИ ПРЕДМЕТНОИ ОБЛАСТИ В ИНФОРМАЦИОННОИ СИСТЕМЕ ОНА ИГРАЕТ ТЕХНИЧЕСКУЮ РОЛЬ*

**Выводы:**

Частотный анализ текста плохо подходит для не больших фрагментов вроде нашего. Поэтому нам приходиться большую часть алфавита подбирать в ручную, либо использовать биграммы и триграммы для лучшего понимания.