CZU: 37.01:004.4=161.1 DOI: 10.36120/2587-3636.v35i1.87-96

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО РЕАЛИЗАЦИИ АЛГОРИТМА ШИФРОВАНИЯ ПРИ ПОМОЩИ КОДОВОГО СЛОВА НА PYTHON

Оксана ГРАДИНАРЬ, кандидат педагогических наук,
https://orcid.org/0000-0003-2628-4251
Государственный Университет им. Алеку Руссо, Бэлць, Молдова
Виолетта БОГДАНОВА, кандидат педагогических наук
https://orcid.org/0000-0003-4140-6317
Государственный Педагогический Университет "Ион Крянгэ", Кишинэу, Молдова
Николай РУССУ, студент
https://orcid.org/0009-0009-8307-6329
Государственный Университет им. Алеку Руссо, Бэлць, Молдова

Аннотация. В статье предложен теоретический и практический материал по шифрованию и дешифрованию текстовых сообщений при помощи шифра кодового слова. Показан пример реализации алгоритма криптографических преобразований указанного шифра на языке программирования Python. Разработка и выполнение кода программы Python осуществлялись в бесплатной интерактивной облачной среде — Google Colab.

Ключевые слова: шифр, открытое сообщение, кодовое слово, язык программирования, интерпретатор.

METHODOLOGICAL RECOMMENDATIONS FOR IMPLEMENTING AN ENCRYPTION ALGORITHM USING A CODEWORD IN PYTHON

Abstract. The article offers theoretical and practical material on encryption and decryption of text messages using a codeword cipher. Is shown an example of the implementation of the algorithm for cryptographic transformations of the specified cipher in the Python programming language. The development and execution of the Python program code was carried out in a free interactive cloud environment — Google Colab.

Key words: cipher, open message, codeword, programming language, interpreter.

RECOMANDĂRI METODOLOGICE DE IMPLEMENTARE A UNUI ALGORITM DE CRIPTARE FOLOSIND UN CUVÂNT DE COD ÎN PYTHON

Rezumat. Articolul oferă material teoretic și practic despre criptarea și decriptarea mesajelor text folosind un cuvânt de cod. Este prezentat un exemplu de implementare a algoritmului pentru transformările criptografice ale cifrului specificat în limbajul de programare Python. Dezvoltarea și executarea codului programului Python a fost realizată într-un mediu cloud interactiv gratuit - Google Colab.

Cuvinte cheie: cifru, mesaj deschis, cuvânt de cod, limbaj de programare, interpretator.

Введение

Анализ научной литературы, представленной многочисленными статьями и материалами конференций, показывает, что вопросами шифрования и дешифрования на сегодняшний день занимаются как национальные, так и

зарубежные авторы: A. Gorceag и D. Afanas [1], I. Popovici [2], A. Zgureanu [3], E. Bădărău [4], Z. Constantinescu и G. Moise [5], Ишмухаметов Ш., Латыпов, Р., Рубцова, Р. и Столов Е. [6], Ларина Н. А. [7], Музыкантский А. И., Фурин В. В. [8] и др. [11, 12, 13].

Широкий интерес к указанной тематике вызван тем, что в течение длительного времени в современном мире остаётся актуальным вопрос об обеспечении сохранности, целостности, подлинности и конфиденциальности информации путём её преобразования с целью исключения возможности доступа посторонним лицам.

Цель данной статьи заключается в реализации криптографического алгоритма шифрования и дешифрования текстовых сообщений (ШДТС) при помощи шифра кодового слова на языке программирования Python в среде Google Colab.

Для достижения цели решены следующие задачи:

1) описан логический алгоритм криптографических преобразований указанного шифра;

2) определены предварительные требования к разработке программы по ШДТС при помощи шифра с использованием кодового слова;

3) представлен программный код реализации алгоритма криптографических преобразований, используя шифр кодового слова.

Алгоритм ШДТС при помощи кодового слова

Последовательность выполнения всех действий при шифровании прямо направлена на предоставление защиты хранимой и передаваемой информации. Таким образом, любой алгоритм шифрования при помощи определённых правил способен преобразовать начальные данные в зашифрованный вид так, что восстановить их может только авторизированное лицо. Данные, которые подлежат шифрованию, называются открытым текстом. Открытый текст необходимо пропустить через определённый алгоритм шифрования, который, представляет собой математические вычисления, осуществляемые над заданной информацией. В настоящее время насчитывается большое количество алгоритмов шифрования, каждый из которых различается по сфере применения и показателям безопасности. Помимо алгоритмов, необходим ещё и ключ шифрования, посредством которого открытый текст преобразуется в зашифрованный фрагмент данных, также известный как шифротекст. Вместо того чтобы отправлять открытый текст заинтересованному лицу (получателю), шифротекст передается по незащищённым каналам связи. И с момента его получения заинтересованным лицом, используется ключ дешифрования для преобразования шифрованного текста обратно в его начальный формат, т. е. в открытый текст. Наглядный пример процесса ШДТС представлен ниже (рис. 1).

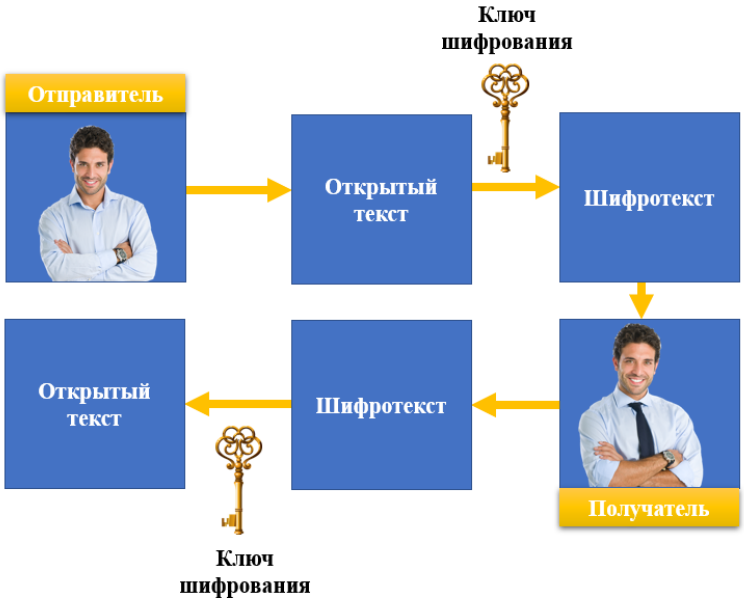

Рисунок 1. Процесс шифрования

Шифр с использованием кодового слова содержит один ключ для шифрования и расшифровки данных. Ключом может быть слово или случайная строка букв. Несмотря на то, что данный шифр имеет свои слабые места, он компенсирует их скоростью и эффективностью.

Рассмотрим алгоритм криптографических преобразований текстовых сообщений при помощи шифра кодового слова на конкретном примере.

Задание. Используя шифр кодового слова, проведите криптографические преобразования (шифрование и дешифрование) над текстовым сообщением: MIJLOACE TEHNICE DE SECURITATE A INFORMAȚIEI при условии, что кодовое слово равно CRIPTARE.

I. Алгоритм шифрования

Во-первых, записываем алфавит языка, на котором будем шифровать открытое сообщение (в нашем случае это английский алфавит).

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Во-вторых, задаём открытое сообщение и кодовое слово. Например:
открытое сообщение: MIJLOACE TEHNICE DE SECURITATE A INFORMAȚIEI.
кодовое слово: CRIPTARE.

По той причине, что алгоритм шифрование планируется проводить на базе букв английского языка, все диакритические знаки, добавленные к буквам для изменения их произношения, необходимо убрать. Тогда открытое сообщение примет вид: MIJLOACE TEHNICE DE SECURITATE A INFORMATIEI.

В-третьих: из кодового слова CRIPTARE отбрасываем каждую вторую повторяющуюся букву. В нашем случае дважды повторяется только буква R. Исключаем вторую и получим CRIPTAE.

В-четвёртых: Вписываем кодовое слово CRIPTAE в начало алфавита, а остальные символы оставляем без изменений.

C	R	I	P	T	A	E	B	D	F	G	H	J	K	L	M	N	O	Q	S	U	V	W	X	Y	Z

В-пятых: После того, как алфавит сдвинут на кодовое слово шифруем сообщение:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C	R	I	P	T	A	E	B	D	F	G	H	J	K	L	M	N	O	Q	S	U	V	W	X	Y	Z

Записываем результат шифрования открытого сообщения путём присваивания каждой букве первой строки предыдущей таблицы каждую букву второй строки. Получим ответ: JDFHLCIT STBKDIT PT QTIUODSCST C DKALOJCSITD.

II. Алгоритм дешифрования

Во-первых, записываем исходные данные:

шифрованное сообщение: JDFHLCIT STBKDIT PT QTIUODSCST C DKALOJCSITD.

кодовое слово: CRIPTARE.

Во-вторых, из кодового слова CRIPTARE отбрасываем каждую вторую повторяющуюся букву. В нашем случае дважды повторяется только буква R. Отбрасываем вторую и получим CRIPTAE.

В-третьих, сдвигаем английский алфавит на кодовое слово CRIPTAE:

C	R	I	P	T	A	E	B	D	F	G	H	J	K	L	M	N	O	Q	S	U	V	W	X	Y	Z

В-четвёртых, записываем английский алфавит в исходном виде.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Записываем результат дешифрования сообщения путём присваивания каждой букве первой строки ниже предложенной таблицы каждую букву второй строки:

C	R	I	P	T	A	E	B	D	F	G	H	J	K	L	M	N	O	Q	S	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Получим ответ: MIJLOACE TEHNICE DE SECURITATE A INFORMATIEI.

Итак, при работе с шифром с использованием кодового слова необходимо учитывать следующие ключевые моменты:

–кодовое слово прописывается впереди алфавита;

–оставшиеся буквы алфавита фиксируются по порядку, пропуская буквы из кодового слова;

–кодовое слово используется при условии исключения каждой второй повторяющейся буквы.

Постановка задачи

Перед написанием программы, которая позволит пользователям шифровать и дешифровать текстовые сообщения при помощи алгоритма шифрования с использованием кодового слова, необходимо сформулировать и описать ряд

характеристик, ожидаемых от конечного продукта. Это позволит решить некоторые принципиальные вопросы, касающиеся общей структуры программы и способов взаимодействия её составляющих элементов (табл. 1).

Таблица 1. Технические требования к разработке программы по ШДТС

1	**Запуск программы**
2	**Ввод выбора операции**
Программа должна выводить приглашение для пользователя о выборе операции: шифрование или дешифрование.	
3	**Обработка выбора операции**
Программа проверяет выбор пользователя и переходит к соответствующей операции.	
4.	**Шифрование текста**
– Программа должна запрашивать текст, который нужно зашифровать; – Программа должна запрашивать ключ, который будет использоваться для шифрования; – После получения текста и ключа, программа должна зашифровать текст с использованием ключа; – Зашифрованный текст выводится на экран.	
5	**Дешифрование текста**
– Программа должна запрашивать зашифрованный текст, который нужно дешифровать; – Программа должна запрашивать ключ, который будет использоваться для дешифрования; – После получения зашифрованного текста и ключа, программа дешифрует текст с использованием ключа; – Дешифрованный текст выводится на экран.	
6	**Требования к входным данным**
Текст для шифрования или дешифрования должен содержать только буквы алфавита.	
7	**Требования к выходным данным**
Программа должна выводить зашифрованный или расшифрованный текст в виде строки.	
8	**Условия и ограничения**
– Длина текста ограничена доступной памятью компьютера; – Длина кодового слова ограничена длиной алфавита (26 символов).	
9	**Обработка ошибок**
– В случае ошибок ввода, таких как пустой текст или ключ, либо если длина ключа превышает 26 символов, программа должна сообщать об ошибке и запрашивать корректный ввод; – В случае введения неправильного выбора операции, программа должна сообщать об ошибке.	
10	**Повторение операций**
После завершения операции шифрования или дешифрования программа должна запросить пользователя о повторения выполнить еще одну операцию. Если пользователь соглашается, цикл повторяется, и программа снова запрашивает выбор операции.	

Реализация алгоритма ШТДС с использованием кодового слова

Криптографический алгоритм ШДТС при помощи кодового слова реализован в Python.

Python — широко используемый интерпретируемый объектно-ориентированный язык программирования высокого уровня с динамической семантикой, используемый для программирования общего назначения. Python бесплатен, открыт и мульти-платформенен [9, с. 4]. Основные направления разработки, классификация, особенности и эффективность данного языка программирования отражены на рисунке 2.

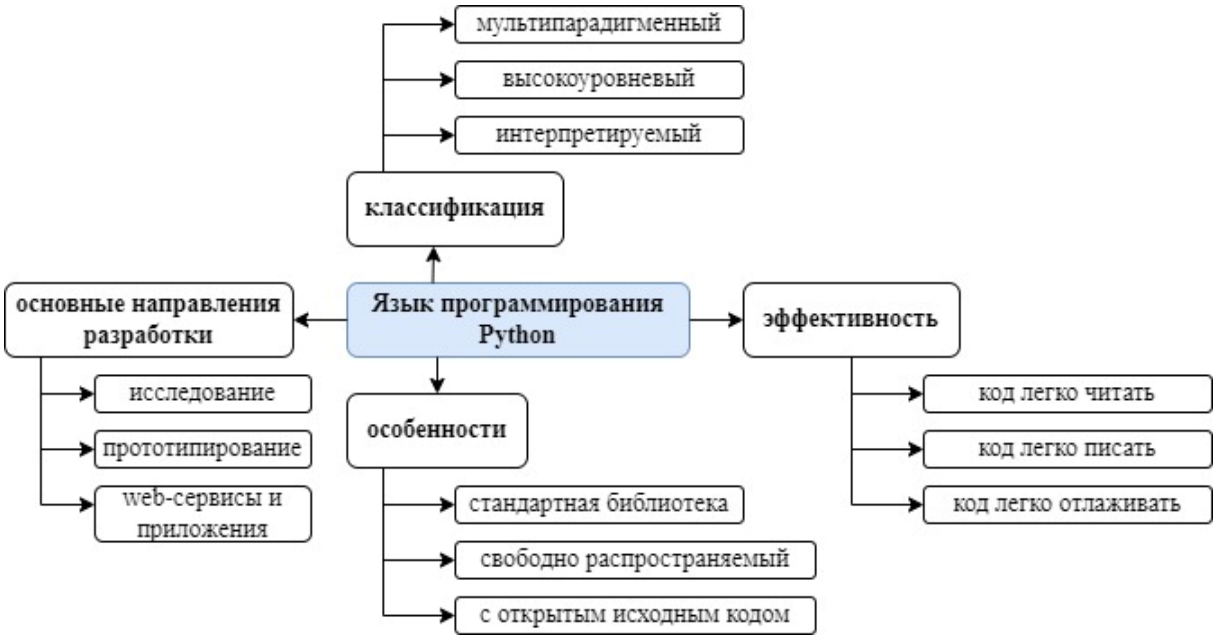

Рисунок 2. Преимущества Python

Работать в Python можно:

- используя локальное устройство. Для этого, на компьютер необходимо установить дистрибутив последней версии www.python.org/downloads/ и текстовый редактор www.sublimetext.com/3;
- используя веб-браузер — среда Google Colab. В этом случае, понадобится аккаунт Google: https://www.google.com/account. Стоит отметить, что в учётных записях Google предусмотрено 15 ГБ бесплатного хранилища, но если в личном кабинете пользователя осталось недостаточно места, то можно создать новый аккаунт Google. Google Colab построен на базе блокнотов Jupyter и поставляется с большим количеством встроенного синтаксиса Python. Это блокнот, который сам по себе представляет собой набор ячеек. Любая данная ячейка содержит либо поясняющий текст, либо исполняемый код (рис. 3).

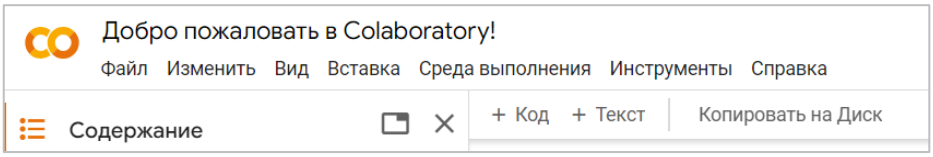

Рисунок 3. Блокнот в Google Colab

Среди преимуществ Google Colab можно выделить следующее:

– в среде не требуется проводить каких-либо дополнительных настроек;
– обеспечен свободный доступ к графическим процессорам;
– удобный обмен.

При работе в Google Colab, периодически необходимо делать локальную копию на Google Диске. В противном случае внесенные пользователем изменения (например, сделанные заметки или написанный код) не будут сохранены.

Листинг кода программы по ШДТС при помощи шифра кодового слова на языке программирования Python представлен ниже.

```
def generate_cipher_map(key):
    alphabet = 'abcdefghijklmnopqrstuvwxyz'
    key = key.lower()
    if len(key) > 26:
        return None
    key_alphabet = ''.join(sorted(set(key), key=key.index))
    cipher_alphabet = key_alphabet + ''.join([ch for ch in alphabet if
ch not in key_alphabet])
    return dict(zip(alphabet, cipher_alphabet))

def encrypt(text, key):
    cipher_map = generate_cipher_map(key)
    if cipher_map is None:
        return None
    text = text.lower()
    encrypted_text = ''.join([cipher_map[ch] if ch in cipher_map else
ch for ch in text])
    return encrypted_text

def decrypt(encrypted_text, key):
    cipher_map = generate_cipher_map(key)
    if cipher_map is None:
        return None
    inverse_cipher_map = {v: k for k, v in cipher_map.items()}
    decrypted_text = ''.join([inverse_cipher_map[ch] if ch in
inverse_cipher_map else ch for ch in encrypted_text])
    return decrypted_text

def main():
```

```
    while True:
        choice = input("Do you want to encrypt or decrypt? (e/d):
").strip().lower()
        if choice == 'e':
            text = input("Enter the text to encrypt: ")
            key = input("Enter the key: ")
            encrypted_text = encrypt(text, key)
            if encrypted_text is not None:
                print("Encrypted text:", encrypted_text)
            else:
                print("Reading error. Check the code word.")
        elif choice == 'd':
            encrypted_text = input("Enter the text to decrypt: ")
            key = input("Enter the key: ")
            decrypted_text = decrypt(encrypted_text, key)
            if decrypted_text is not None:
                print("Decrypted text:", decrypted_text)
            else:
                print("Error during decryption. Check the code word.")
        else:
            print("Invalid choice. Please enter 'e' to encrypt or 'd'
to decrypt.")

        cont = input("Do you want to continue? (y/n):
").strip().lower()
        if cont != 'y':
            break
if __name__ == "__main__":
    main()
```

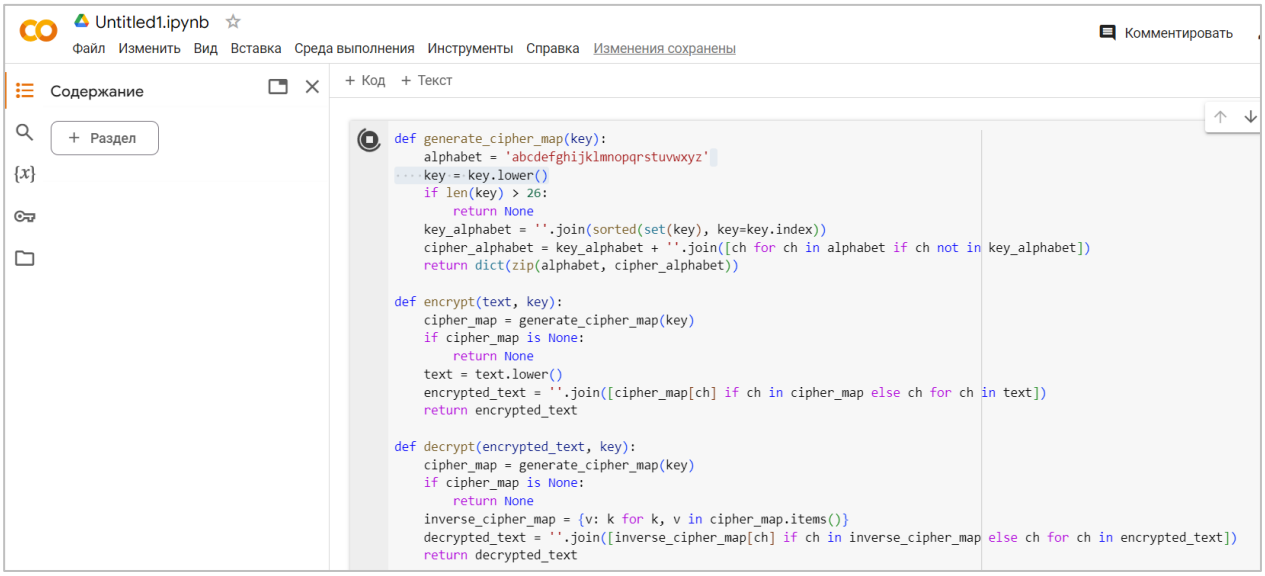

Рисунок 4. Фрагмент кода ШДТС при помощи кодового слова в Google Colab

Фрагмент кода программы по ШДТС при помощи шифра кодового слова на языке программирования Python в Google Colab представлена на рисунке 4.

Указанная программа выводит приглашение о выборе операции: шифрование или дешифрование текстовых сообщений. Затем, пользователю необходимо нажать букву “e” для шифрования или “d” для дешифрования. В случае, если пользователь решает не выполнять больше операций, ему позволено выбрать завершение работы, введя “n” при запросе повторения операций (рис. 5).

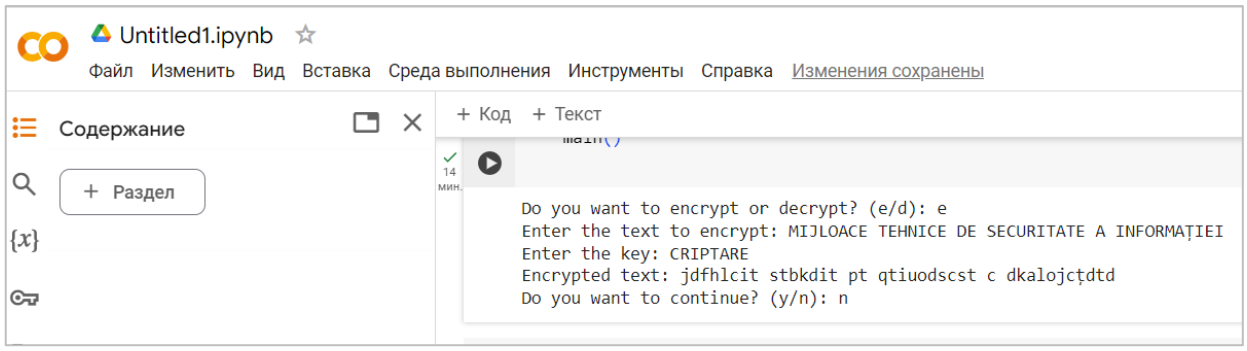

Рисунок 5. Результат запуска кода в Google Colab

Выводы и рекомендации

В рамках статьи подробно рассмотрен алгоритм ШДТС при помощи шифра кодового слова, разработана программа средствами языка Python в среде Google Colab, демонстрирующая работу данного алгоритма.

Библиография

1. GORCEAG, A.; AFANAS, D. Repere teoretice în criptografia pre-computaţională. In: *Materialele conferinţei ştiinţifice a studenţilor*, 1-2 octombrie 2019, Chişinău: Tipografia Universităţii de Stat din Tiraspol, 2019, Ediția 68, pp. 130-132. ISBN 978-9975-76-280-9.
2. POPOVICI, I. Criptografia, metoda pentru asigurarea securităţii tranzacţiilor de date. In: *Analele Ştiinţifice ale Universităţii de Stat”Bogdan Petriceicu Hasdeu” din Cahul*, 2012, nr. 8, pp. 162-171. ISSN 1875-2170.
3. ZGUREANU, A. *Criptarea şi securitatea informaţiei*. Note de curs. Chișinău, 2013.
4. BĂDĂRĂU, E. Metode şi practici de securizare a informaţiei. In: *Relaţii internaţionale. Plus*, 2016, nr. 1(9), pp. 141-146. ISSN 1857-4440.
5. CONSTANTINESCU, Z. ; MOISE, G. *Criptarea informaţiei: ghid practic.* - Ploieşti: Editura Universităţii Petrol-Gaze din Ploieşti, 2013. 119 p. ISBN 978-973-719-522-7.

6. ИШМУХАМЕТОВ, Ш. Т.; ЛАТЫПОВ, Р. Х.; РУБЦОВА, Р. Г.; СТОЛОВ, Е. Л. *Введение в теорию кодирования и криптографию: Учебное пособие*. Казань: Казанский ун-т, 2021. 211 с.
7. ЛАРИНА, Н. А. *Защита информации. Криптология: Методическое пособие для бакалавров направления подготовки 09.03.01 «Информатика и вычислительная техника»*. Рубцовск: Рубцовский индустриальный институт, 2014. 56 с.
8. МУЗЫКАНТСКИЙ, А. И.; ФУРИН, В. В. *Лекции по криптографии*. М.: МЦНМО, 2013. 2-е изд., стереотип. 68 с.
9. КОСИЦИН, Д. Ю. *Язык программирования Python: учеб.-метод. пособие*. Минск: БГУ, 2019. 136 с. ISBN 978-985-566-746-0.
10. STAN, A. *Introducere în Python folosind Google Colab*. Cluj-Napoca: UTPRESS, 2022. 245 p. ISBN 978-606-737-593-0.
11. АХМЕТОВ, Б. С.; КОРЧЕНКО, А. Г.; СИДЕНКО, В. П. *Прикладная криптология: методы шифрования: учебное пособие*. Алматы: КазНИТУ имени К. И. Сатпаева, 2015. 496 с. ISBN 978-601-228-879-7.
12. НИКИФОРОВ, С. Н. *Методы защиты информации. Шифрование данных: Учебное пособие.* Лань, 2019 г. 160 с. ISBN: 978-5-8114-3097-0.
13. БАРИЧЕВ, С. Г.; ГОНЧАРОВ, В. В.; СЕРОВ, Р. Е. *Основы современной криптографии: Учебный курс*. М: 3-е изд., стереотип., 2011. 176 с. ISBN 978-5-9912-0182-7.