Использованный метод дешифровки делает невозможным чтение сообщения на другом девайсе. Чтобы дешифровать сообщение, следует ввести зашифрованную строку и ее шифр.

Таким образом, разработанный алгоритм, реализованный в программе, обеспечивает высокий уровень защиты данных против дешифрования и возможной модификации, защищенность информации основывается только на знании ключа, малое изменение исходного текста или ключа приводит к значительному изменению шифрованного текста, экономичность реализации алгоритма при достаточном быстродействии.

ЛИТЕРАТУРА

1. Н. В. Пацей. Основы алгоритмизации и программирования: учеб.-метод. пособие для студентов специальности «Информационные системы и технологии» / Н. В. Пацей. – Минск: БГТУ, 2010. – 289 с.

2. Ф. Циммерман. Введение в криптографию / Ф. Циммерман. – PGP Corporation, 2004. – 18 с.

УДК 004.4

Магистрант А.Г. Оганесян
Науч. рук. доц. Н.Н. Пустовалова
(кафедра информационных систем и технологий, БГТУ)

АНАЛИЗ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ БИБЛИОТЕКИ PANDAS НА ЯЗЫКЕ PYTHON

Учет личных расходов является одним из инструментов оптимизации личных финансов. Система, которая смогла бы вести учет личных расходов и на основании собранных данных выдавать пользователю информацию о его тратах является актуальной и будет всегда востребована. Для обработки и анализа данных при решении данной задачи можно воспользоваться библиотекой pandas.

Pandas – это высокоуровневая Python библиотека для анализа данных. Она построена поверх низкоуровневой библиотеки NumPy, которая написана на языке Си, что является большим плюсом для производительности. С помощью pandas можно как анализировать данные, так и в связке с matplotlib визуализировать их.

Чтобы эффективно работать с pandas, необходимо освоить самые главные структуры данных библиотеки: DataFrame и Series[1].

Объект Series представляет собой объект, похожий на одномерный массив, но отличительной его чертой является наличие ассоциированных меток (индексов), вдоль каждого элемента из списка. Если индекс явно не задан, то pandas автоматически создаёт RangeIndex от

0 до N-1, где N – общее количество элементов. Доступ к элементам объекта Series возможен по их индексу.

Объект DataFrame лучше всего представить в виде обычной таблицы, поскольку он является табличной структурой данных. В любой таблице всегда присутствуют строки и столбцы. Столбцами в объекте DataFrame выступают объекты Series, строки которых являются их непосредственными элементами.

В задаче анализа расходов с помощью pandas можно получить такие востребованные данные, как: расходы пользователя за некоторое время, предварительно сгруппированные по категориям; расходы пользователя по определенной категории за каждый месяц; все расходы пользователя помесячно, без разделения на категории.

Для выполнения первой задачи (отображения сгруппированных по категориям расходов) необходимо считать данные из файла с расходами в DataFrame с помощью функции read_csv(), далее с помощью функции groupby() необходимо сгруппировать расходы по атрибуту «категория». Теперь все что осталось, это получить Series для колонки «amount», вызвать функцию sum(), после чего в нашем распоряжении будет новый объект типа DataFrame (рис. 1). Останется только визуализировать его.

```
import pandas

df = pandas.read_csv('expenses.csv', parse_dates=True, index_col='date')


new_df = df.groupby('category')['amount'].sum()
plot = new_df.plot(kind='barh', grid=True, legend=True)
plot.get_figure().savefig("all_by_cat.png")
```

Рисунок 1– Исходный код визуализации расходов по категориям

На рис. 2 представлена визуализация расходов по категориям.

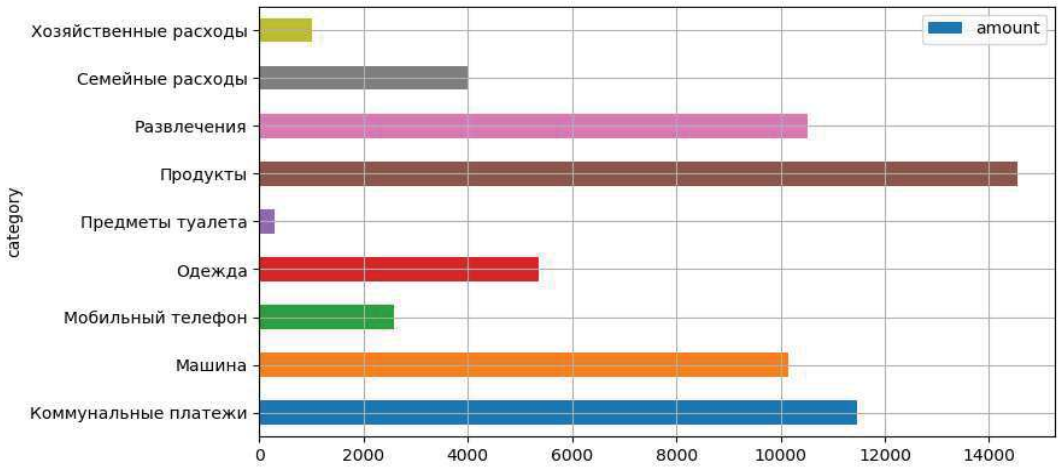

Рисунок 2– Визуализация расходов по категориям

Чтобы отобразить расходы по определенной категории (например, для категории «Развлечения») помесячно для начала необходимо отфильтровать DataFrame по нужному значению нужной колонки, далее с помощью функции resample() переформировать DataFrame помесячно. Далее все, как и в предыдущем примере.

Таким образом, библиотека pandas поддерживает все самые популярные форматы хранения данных, позволяет их анализировать по различным параметрам и визуализировать полученные результаты. Использование данного программного продукта способствует эффективному решению задачи учета личных расходов пользователя.

ЛИТЕРАТУРА

1. Документация pandas [Электронный ресурс]. – Режим доступа: https://pandas.pydata.org/pandas-docs/stable/index.html – (Дата обращения: 15.04.2019).

УДК 004.056.55

Студ. К.А. Ермаков
Науч. рук. проф., д.т.н. П.П. Урбанович
(кафедра информационных систем и технологий, БГТУ)

ОСОБЕННОСТИ ПРАКТИЧЕСКОЙ РЕАЛИЗАЦИИ КВАНТОВОЙ КРИПТОГРАФИИ НА ОСНОВЕ ПРОТОКОЛА БЕННЕТА

Основной задачей криптографии является зашифрование/расшифрование передаваемых данных. К другим задачам относятся: генерация и распределение ключей, аутентификации сторон и т. п. [1].

Задача согласования ключевой информация, предложенная Диффи и Хеллманом, относится к классическим методам асимметричной криптографии. Согласование ключей может основываться и на технологиях искусственных нейронных сетей [2].

В работе рассматриваются основные идеи относительно нового направления – квантовой криптографии (КК). Задача КК – секретное распределение симметричных (одинаковых) ключей между легитмиными пользователями. В отличие от традиционной криптографии, опирающейся на математические методы, квантовая криптография основывается на фундаментальных законах квантовой механики [3, 4]. При попытке «подслушать»/измерить квантовое состояние оно неизбежно меняется, а, значит, если кто-то попытается скопировать ключ во время его распределения, об этом станет известно легитимным пользователям.