УДК 681.004.89:164.053 https://doi.org/10.35546/kntu2078-4481.2021.1.13

N.V. KORNILOVSKA
Kherson national technical university
ORCID: 0000-0002-8331-8027
S.V. VYSHEMYRSKA
Kherson national technical university
ORCID: 0000-0002-6343-7512
M.O. KOLMYKOV
Kherson national technical university

DEVELOPMENT OF PYTHON ELECTRONIC MESSAGE INFORMATION PROTECTION SYSTEM USING THE PYCHARM WORKING AREA

The information security is one of the widespread problems which the modern society is facing. The reason for the aggravation of this problem is the large-scale use of automated means of accumulation, storage, processing and transmission of information. The appearance of global computer networks has made it easy to access information for both individuals and large organizations. However, this achievement has led to a number of complex problems, including the problem of information security. The solution to the problem of information protection is associated with guaranteed information availability, its integrity and confidentiality.

The most significant threats to data security are: 1) non-automated access to information; 2) non-automated change of information; 3) non-automated access to networks and services; 4) other network attacks, such as the recurrence of previously intercepted transactions (groups of commands) and denial-of-service attacks. A common method of protection in computer systems is the use of passwords which is more suitable for protecting access to computing resources than for protecting information itself. A password is a kind of shield that separates legitimate users from third party users, after which the authorized user gets the access to all information. The system of information protection involves the use of various methods of organizational-administrative, technological, technical, legal, moral-ethical nature. In addition, we can identify information technologies that include cryptographic and software means of information security.

Interactive environments are vulnerable from the data security position. An example of interactive environments is any of the systems with communication capabilities, such as e-mail, computer networks, the Internet. The information transmission through communication channels in the Internet is often risky. Being aware of effective security measures when using e-mail is becoming an urgent need for both organizations and citizens.

Keywords: Information security, cryptography, e-mail.

Н.В. КОРНІЛОВСЬКА
Херсонський національний технічний університет
ORCID: 0000-0002-8331-8027
С.В.ВИШЕМИРСЬКА
Херсонський національний технічний університет
ORCID: 0000-0002-6343-7512
М.О. КОЛМИКОВ
Херсонський національний технічний університет

РОЗРОБКА СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ЕЛЕКТРОННОГО ПОВІДОМЛЕННЯ МОВОЮ PYTHON З ВИКОРИСТАННЯМ СЕРЕДИ РОЗРОБНИКА PYCHARM

Інформаційна безпека - одна з головних проблем, з якою стикається сучасне суспільство. Причиною загострення цієї проблеми є широкомасштабне використання автоматизованих засобів накопичення, зберігання, обробки і передачі інформації. Поява глобальних комп'ютерних мереж зробила простим доступ до інформації, як окремим громадянам, так і великим організаціям. Однак це досягнення спричинило за собою цілий ряд складних проблем, в тому числі і проблему захисту інформації. Рішення проблеми інформаційного захисту пов'язане з гарантованим забезпеченням доступності інформації, її цілісності і конфіденційності (секретності).

Найбільш значні загрози безпеки даних представляють: 1) неавтоматизований доступ до інформації; 2) неавтоматизована зміна інформації; 3) неавтоматизованих доступ до мереж і сервісів; 4) інші мережеві атаки, наприклад повтор перехоплених раніше транзакцій (групи команд) і атаки типу «відмова в обслуговуванні». Поширений в комп'ютерних системах спосіб захисту - використання паролів - більш придатний для захисту доступу до обчислювальних ресурсів, ніж для захисту інформації. Пароль

- своєрідний екран, що відгороджує законних користувачів від сторонніх, пройшовши який санкціонований користувач отримує доступ до всієї інформації.

Система захисту інформації передбачає використання різних методів, що носять організаційно-адміністративний, технологічний, технічний, правової, морально-етичний характер. Крім них можна виділити інформаційні технології, що включають криптографічні та програмні засоби захисту інформації.

Інтерактивні середовища уразливі з позицій безпеки даних. Прикладом інтерактивних середовищ є будь-яка з систем з комунікаційними можливостями, наприклад електронна пошта, комп'ютерні мережі, Інтернет.

Передача інформації по каналах зв'язку в Інтернеті часто схильна до ризиків. Знання дієвих заходів захисту при використанні електронної пошти стає нагальною потребою і для організацій, і для громадян. Ризиків втрати, перекручування, заміни достовірних даних помилковими схильні до листування, дані адресної книги.

Ключові слова: Інформаційна безпека, криптографія, електронна пошта.

Н.В. КОРНИЛОВСКАЯ
Херсонский национальный технический университет
ORCID: 0000-0002-8331-8027
С.В.ВИШЕМИРСКАЯ
Херсонский национальный технический университет
ORCID: 0000-0002-6343-7512
М.О. КОЛМИКОВ
Херсонский национальный технический университет

РАЗРАБОТКА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ЭЛЕКТРОННОГО СООБЩЕНИЯ НА ЯЗЫКЕ PYTHON С ИСПОЛЬЗОВАНИЕМ СРЕДЫ РАЗРАБОТЧИКА PYCHARM

Информационная безопасность - одна из главных проблем, с которой сталкивается современное общество. Причиной обострения этой проблемы является широкомасштабное использование автоматизированных средств накопления, хранения, обработки и передачи информации. Появление глобальных компьютерных сетей сделала простым доступ к информации, как отдельным гражданам, так и крупным организациям. Однако это достижение повлекло за собой целый ряд сложных проблем, в том числе и проблему защиты информации. Решение проблемы информационной защиты связано с гарантированным обеспечением доступности информации, ее целостности и конфиденциальности (секретности).

Наиболее значительные угрозы безопасности данных представляют: неавтоматизированный доступ к информации; неавтоматизированная изменение информации; неавтоматизированных доступ к сетям и сервисам; другие сетевые атаки, например повтор перехваченных ранее транзакций (группы команд) и атаки типа «отказ в обслуживании». Распространен в компьютерных системах способ защиты - использование паролей - более пригоден для защиты доступа к вычислительным ресурсам, чем для защиты информации. Пароль - своеобразный экран, отгораживает законных пользователей от посторонних, пройдя который санкционирован пользователь получает доступ ко всей информации.

Система защиты информации предполагает использование различных методов, носят организационно-административный, технологический, технический, правовой, морально-этический характер. Кроме них можно выделить информационные технологии, включающие криптографические и программные средства защиты информации.

Интерактивные среды уязвимы с точки зрения безопасности данных. Примером интерактивных сред является любая из систем с коммуникационными возможностями, например электронная почта, компьютерные сети, Интернет.

Передача информации по каналам связи в Интернете часто подвержена рискам. Знание действенных мер защиты при использовании электронной почты становится насущной необходимостью и для организаций, и для граждан. Рисков утраты, искажения, замены достоверных данных ошибочными подвержены переписки, данные адресной книги.

Ключевые слова: информационная безопасность, криптография, электронная почта.

Problem Statement

Interactive environments are vulnerable from a data security position. An example of interactive environments is any of the systems with communication capabilities, such as e-mail, computer networks, the Internet. Email is any type of communication used by computers and modems. The most vulnerable points in e-mail are the sender's outgoing e-mail point and the recipient's mailbox. Each of the e-mail software packages allows archiving incoming and outgoing messages at any other address, which can lead to abuse by attackers [1]. Modern users do not want to give up such a convenient means of communication as e-mail, but the risks are very high. Email needs to be protected from various threats. At a modern enterprise, e-mail serves as a messenger and a telephone line, which is why the attackers often use it as a springboard for further attacks on corporate infrastructure.

Email security is a task of an utmost importance. As at every enterprise the employees correspond with customers and partners, so e-mail contains a lot of information that can be used by competitors and fraudsters. They can forge a letter, add malware and malware links into it – there are a lot of such examples [1].

The aim of this research is to develop a way to combine with the maximum efficiency the Python 3.7 programming language toolbox with the capabilities of the programming working area PyCharm; identify and evaluate the most vulnerable points when sending e-mails; get a convenient and simple functional that will simultaneously encrypt with different methods (the Caesar encryption algorithm, the Vigenère encryption algorithm, the XOR encryption algorithm, Bacon's encryption algorithm and encryption by own algorithm) and send them by e-mail.

Analysis of the latest researches and publications

Personal interests in the information sphere consist of the realization of the constitutional human and civil rights to the access of information, the use of information in the interests of not prohibited by law activity, physical, spiritual and intellectual development, as well as the protection of information that provides personal security [2].

The rules for secure correspondence are given in Fig. 1.

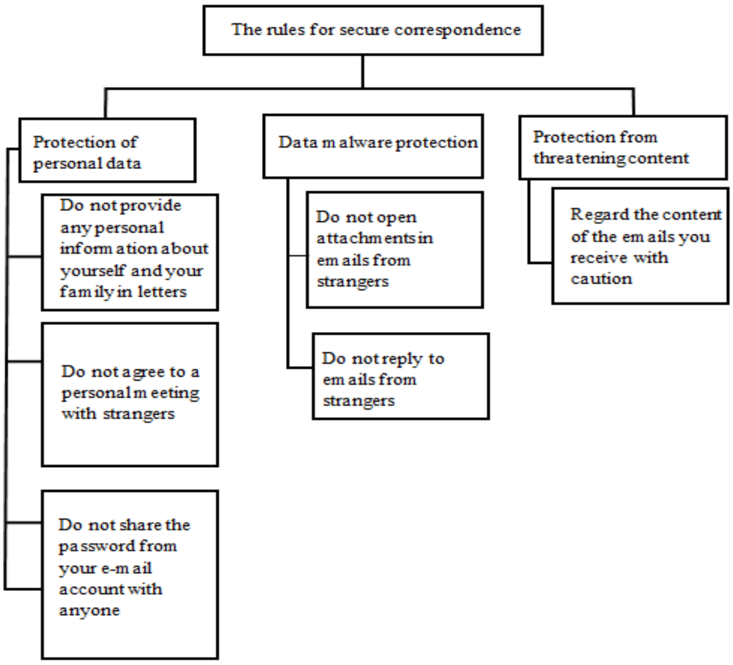

The rules for secure correspondence
Protection of personal data
Do not provide any personal information about yourself and your family in letters
Do not agree to a personal meeting with strangers
Do not share the password from your e-mail account with anyone
Data malware protection
Do not open attachments in emails from strangers
Do not reply to emails from strangers
Protection from threatening content
Regard the content of the emails you receive with caution

Fig. 1. The rules for secure correspondence

Cryptographic tools are most often used for mail security, but experts also recommend other technologies. Email security tools appear as particular applications, browser extensions, and secure resources that offer to use email in a way that avoids all major threats. Sometimes the problem can be solved by installing a plugin (extension), which allows providing asymmetric or symmetric encryption [3].

Almost all common tools have disadvantages in terms of security, namely:

• choosing an encryption algorithm that does not provide reliable protection of information transmitted by e-mail channels. This is sometimes due to the fact that the national legislation of the country of stay or registration does not recommend using high-reliability encryption algorithms to ensure access to confidential correspondence;

• system or non-system failures when using secure data transfer protocols or cryptographic security tools when using e-mail;

• backdoors in cryptographic algorithms, undeclared capabilities of programs that allow developers to decrypt the information;

• actions of malicious, viral programs that intercept data on its way or on the server [4].

Most of the problems of e-mail security systems are known, so the developers use all means to fight them when creating security measures architecture. If it is assumed that the danger may be observed from the letter recipient, who may use it for further dissemination of information, then the programs that allow only reading the letter, but do not allow copying it or using it for other purposes are used. Such programs are called viewers, they can be browser add-ons. The disadvantage of these software tools is that you can always take a screenshot of a short letter and then use the data to form a document. Similar options of restricting data copying are implemented in some messengers [4].

The choice of software solutions is based on understanding of what threats the e-mail system of an individual or company needs to be protected from and what mechanisms should be used for this purpose. In addition to special programs designed to protect data transmitted by open channels, there are common tools, namely:

• email antiviruses. They scan incoming correspondence for malware, as well as perform e-mail protection tasks;

• programs that detect spam and filter the prohibited mailings.

The functional of the specified program types is based on using e-mail protocols POP3, SMTP, NNTP, IMAP. Intercepting invalid correspondence types and their investigation is automatic. Plugins built into browsers are also used for this purpose. Antivirus software that filters the unwanted traffic and protects e-mail from spam is automatically built in Microsoft Office Outlook and The Bat! modules [4].

PGP Mail browser plugin. It is a cryptographic data protection tool that offers an asymmetric encryption mechanism for the data (with public and private key) transmitted by e-mail. Protection is provided on the user's side. PGP Mail is supported by all major browsers, including Firefox, Chrome, Opera, Safari. The best results in the field of computer information protection can be achieved if TOR is used together with the plugin. But it will be difficult to follow this recommendation if the plugin is used by an inexperienced user. The disadvantages of the plugin include the ability to use only popular browsers.

SecureGmail browser plugin. This extension offers users a symmetric encryption mechanism, the keys do not differ for the email sender and recipient. This implies that the correspondence participants trust each other completely. It is advised to use this plugin only when a small number of participants take part in the correspondence. As the number of generated keys will increase within the expansion of the circle of communication. It is no purpose to store a lot of keys, it contradicts the rules of information security.

Encrypted Communication browser plugin. The EC extension has a similar disadvantage, it can only be used with Firefox browser. The plugin offers the same not very convenient symmetric encryption system with the second public key, which limits the number of correspondents to 2-3. On the other hand, using simple applications does not create complex tasks for users who only need to send and receive an email without thinking about the degree of its confidentiality. There is no need to generate key certificates, it is enough to create one and pass it to correspondence partners [5].

Enigmail email client plugin. This extension is not used for the browser, but for the email client. The plugin has different functions compared to the previous ones, but is also designed to protect against leaks using cryptographic means. To make the module work, you must first install the GnuPG program, which is also not always convenient. But in the end, the user will get an asymmetric encryption system, which increases the level of security. The disadvantage of the Enigmail plugin is the need to use the knowledge required to generate the key [6].

Goal Setting

In this research we will make a comparative analysis of a number of software products designed for cryptographic information protection. We will justify which one to choose in a particular case. We will study a new version of Python3.7, which includes a number of optimizations. We will practically process the PyCharm working area, which to our mind is one of the best full-featured, specialized and all-purpose IDEs for Python development. We will examine and implement different concepts of encryption methods: Caesar's cipher; the Vigenère cipher; Bacon's cipher; XOR cipher.

We will create and implement our own encryption method. The uniqueness of this method of encryption will be that for encryption / decryption you need to know only the algorithm principle. The final practical result of our research will be creating our own software product, the "Encryptor" shell, which has a convenient and simple interface and will allow not only encrypting and decrypting with several methods to choose from but also sending an encrypted message via email without leaving this shell.

Presentation of research material

The mailbox protection task can be solved using modern security tools. Encrypting messages will protect a mailbox in most cases, but its application requires certain skills. Solving this task will be a good solution for corporate clients who are thinking about maintaining the external correspondence security. An additional solution, which is mandatory for use, is the archiving of all correspondence, and archives must be protected with a strong password.

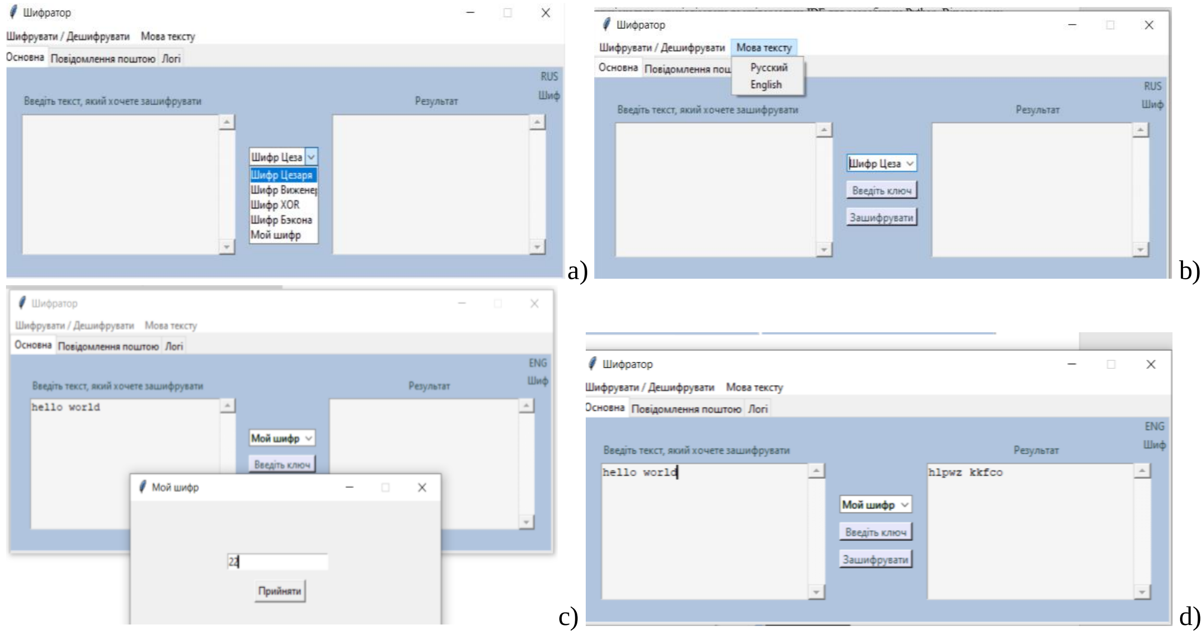
In this research we have compared a number of software products designed to protect information cryptographically. Anyone who is seriously concerned about the security of their confidential information faces the task of selecting software for cryptographic data protection, as encryption today is one of the most reliable ways to prevent unauthorized access to important documents, databases, photos and any other files.

The problem is that in order to make a competent choice it is necessary to understand all aspects of how cryptographic products work. First, these are the encryption algorithms available in the product. Second, these are the ways to authenticate the information owners. Third, these are the ways to protect the information. Fourth, these are the additional features and capabilities. Fifth, this is the manufacturer’s authority and popularity, as well as his possession of certificates for the development of encryption tools. And that is not all that may be important when choosing a cryptographic protection system. A significant disadvantage of the considered software products is their high cost and certain compatibility issues with different versions of operating systems. In our research, we have come to the conclusion that it is better to create your own software product that will meet all our requirements: being free, giving a choice of encryption methods, providing a simultaneous sending of an encrypted message by e-mail.

As for the programming language we have chosen in our research, it should be noted that each new version of Python includes a number of optimizations. Python 3.7 is no exception, so we can take advantage of some improvements, including [7]:

- Lower hardware system requirements when using a variety of methods from a standard library.
- In general, execution of methods happens 20% faster.
- 10-30% improvement of Python startup time.
- Imports are introduced 7 times faster.

The result of these optimizations is obvious – Python 3.7 works faster. This is the fastest version of CPython at the moment. It should also be added that the PyCharm working area is one of the best, full-featured, specialized and all-purpose for Python development. It has many features that save time helping us with routine tasks. In the main window of the software product created by us we select the encryption algorithm, data-entry language, and encryption key (Fig. 2 a, b, c, d).



hello world

22

hello world

hlpwz kkfco

Fig.2. The main window of the “Encryptor” program

The implementation of the Caesar encryption algorithm. A Caesar cipher is a kind of substitution cipher in which each character in the text is replaced by a character that is at some constant number of positions to the left or to the right of it in the alphabet. The same way the decryption process is performed here, there are checkboxes that define this function. There is also a try ... except exception handler that tracks errors such as IndexError and ValueError, which occur when entering the wrong key format, as well as in the absence of the key.

The implementation of the Vigenère encryption method. The Vigenère cipher is a method of polyalphabetic encryption of letter text using a keyword. This method is a simple form of multi-alphabetic substitution. The same way the decryption process is performed within this method, the action is determined by the appropriate checkbox. It contains the try ... except error handler to determine the incorrect key format or its absence.

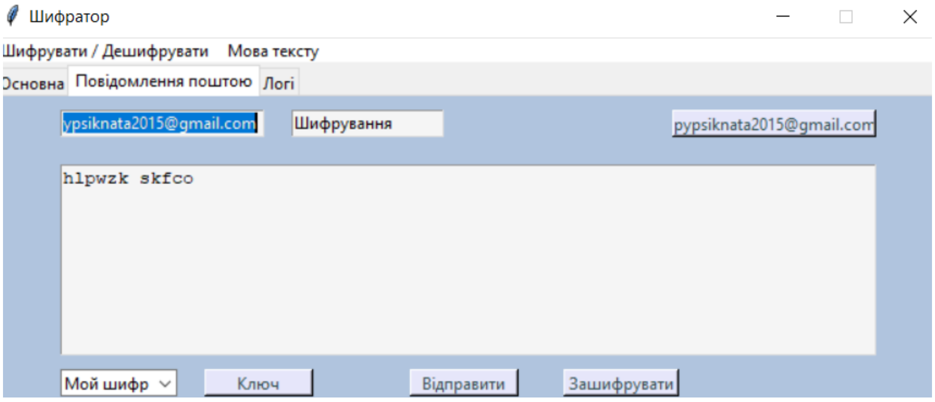
The implementation of XOR encryption algorithm. “Gamma xoring” is a method of symmetric encryption, which consists of “overlaying” a sequence made of random numbers on plaintext. A sequence of random numbers is called a gamma sequence and is used to encrypt and decrypt data. Summing is usually performed in any finite field. It contains try ... except error handler to detect the errors.

The implementation of the Bacon's encryption method. Bacon's cipher is a method of concealing a secret message, invented by Francis Bacon in the early seventeenth century. He developed ciphers that would allow transmitting secret messages in plain text so that no one would know about these messages. The cipher is based on the binary encoding of the alphabet with the characters "A" and "B", which can be compared with "0" and "1". Then the secret message is "hidden" in the open text, using one of the ways of hiding messages.

The implementation of our own encryption method. This encryption method is based on the first letter. It is a more improved version of a Caesar cipher, but we have borrowed from a Caesar cipher only the movement of the symbol to a certain step. If in a Caesar cipher a step is specified, then in this case for decryption it is only required to know the encryption method. Only the first letter is required for encryption. Each next letter, except the first (it remains unchanged), is encrypted on the basis of the previous one. The encryption step of each letter is determined by the location of the previous letter of the given text in the alphabet. The following is a part of the code to describe our own encryption method.

```
def my_encrypt ():
if tab_control.index ( 'current') == 0:
message = LeftText.get (1.0, END)
 else:
message = msgtext.get (1.0, END)
language = alphabetENG
message = message.lower ()
 result = [message [0]]
 word1 = message [1:]
pred = ord (message [0]) – 97
 for i in word1:
if i in language:
num = ord (i) – 97
if state_mode:
num1 = num + pred
pred = num
else:
num1 = num – pred
pred = num1
 result.append (language [num1])
 else:
result.append (i)
 encrypted = '' .join (i for i in result)
result.clear ()
 insert_text (encrypted)
```

The interface for sending an e-mail is given in Fig. 3.



ypsiknata2015@gmail.com

Шифрування

pypsiknata2015@gmail.com

```
hlpwzk skfco
```

Fig.3. Interface for sending an e-mail

Next, we provide a part of the code to describe the function of sending an e-mail [7,8].

```
def msg_send ():
 "" " Sending message to the specified email address button" ""
            try:
             msg = MIMEMultipart ()
            msg [ 'From'] = email
            msg [ 'To'] = msgto.get ()
            msg [ 'Subject'] = subjectentry.get ()
            msg.attach (MIMEText (msgtext.get (1.0, END), 'plain'))
             server.login (msg [ 'From'], password)
            server.sendmail (msg [ 'From'], msg [ 'To'], msg.as_string ())
            error.showinfo ( 'Mail',MESSAGE is sent!')
            except smtplib.SMTPAuthenticationError:
             error.showerror ( 'Error', 'incorrect login or password')
```

The message is sent thanks to the smtlib and email library.

Conclusions

The conducted research has revealed that the most vulnerable points in e-mail are the sender’s outgoing e-mail point and the recipient’s mailbox.

The mailbox protection task can be solved using modern security tools. Encrypting messages will protect a mailbox in most cases, but its application requires certain skills. Solving this task will be a good solution for corporate clients who are thinking about maintaining the external correspondence security. An additional solution, which is mandatory for use, is the archiving of all correspondence, and archives must be protected with a strong password.

One of the main practical tasks of this research was to study and combine the modern software and hardware methods tools of information protection with the ability to create our own software product for cryptographic method of information confidentiality protection.

In the process of practical implementation of the set tasks, we have considered and implemented various concepts of encryption methods: a Caesar cipher; the Vigenère cipher; Bacon’s cipher; XOR cipher.

In this research we have created and implemented our own method of encryption. The uniqueness of this method of encryption is that for encryption / decryption you need to know only the algorithm principle. The final practical result of our research has been the creation of our own software product, the “Encryptor” shell, which has a convenient and simple interface. It also provides the user not only with services of encrypting and decrypting with several methods to choose from, but also sending an encrypted e-mail without leaving this shell. The program has been implemented using the Python programming language in the PyCharm working area.

References

1. Gutman B., Begville R. Safety policy when working on the Internet – a technical guide. – Available at: https://www.studmed.ru/gutman-b-begvill-r-politika-bezopasnosti-pri-rabote-v-internete-tehnicheskoe-rukovodstvo_5934bf323ba.html

2. Bashlam P.M, Babash A.V, Baranova EK Information security: a textbook, Moscow, Izd.tsentr EAOI, 2010, 376 p.

3. Babash A.V Cryptographic and theoretical-automatic aspects of modern information protection. Cryptographic methods of protection, Moscow, Publishing Center EAOI, 2009. – 414 c.

4. Domarev V.V. Title: Information Technology Security. Methodology of creating protection systems. Publisher: TID Dia Soft, 2006, 688 p.

5. Nielsen M., Chang I. Quantum calculations and quantum information / Per. from English Moscow, 2006; Gomonai O.V Lectures on quantum informatics: Textbook. way. V., 2006; Vasiliu E.V. Stability of quantum protocols for the distribution of keys such as "preparation-measurement" // *Georgian Electronic Scientific J .*: Computer Science and Telecommunications. 2007. № 2 (13);

6. Kilin S. Ya., Khoroshko D.B, Nizovtsev A.P. Quantum cryptography: Ideas and practice. Minsk, 2008; Korchenko O.G, Vasiliu E.V, Hnatiuk S.O. Modern quantum technologies of defense information // *Information protection*. 2010. № 1.

7. Fedorov, D. Yu. Programming in the language of the high level of Python: a textbook for the applied bachelor's degree / D. Yu. Fedorov, Moscow, Publishing Yrayt, 2017,126 p.

8. CPython implementation detail:- Available at: https://docs.python.org/3.7/using/cmdline.html#id5