TASHKENT STATE UNIVERSITY OF ECONOMICS

International journal of topics

INNOVATION SCIENCE AND TECHNOLOGY

Scopus || Electronic journal specializing in Scopus

ISSUE 11

Acceptance of papers **November, 2025**

Acceptance of papers

Published monthly

Topics

economics, technology, social sciences

ISSN 3060-5229

Electronic publication, Issue 11. 52 pages.
Approved for publication on November, 2025.

THE SCIENTIFIC-POPULAR ELECTRONIC JOURNAL **"INNOVATION SCIENCE AND TECHNOLOGY"** HAS BEEN REGISTERED UNDER THE NUMBER **C-5669633** BY THE AGENCY FOR INFORMATION AND MASS COMMUNICATIONS (AOKA) OF THE REPUBLIC OF UZBEKISTAN, EFFECTIVE FROM OCTOBER 9, 2024.

CONTACTS

Phone: **+998 50 737 87 88**

Website: https://ist-journal.uz

Email: innovationist2025@gmail.com

The scientific electronic journal “Innovation Science and Technology” has been included in the list of scientific publications recommended for the publication of main scientific results of dissertations for the award of PhD and DSc degrees in economics and technical sciences, in accordance with the Resolution No. 370 of the Presidium of the Higher Attestation Commission of the Republic of Uzbekistan, dated May 8, 2025.

Editorial board:

CONTENTS

"CREATING AN ALGORITHM AND SOFTWARE TOOL FOR PERSONAL IDENTIFICATION USING FACIAL SCANNING TO PROTECT THE OPERATING SYSTEM"

Usmonov Maxsud Tulqin o‘g‘li
Master’s student at the National University of Uzbekistan
Email: maqsudu32@gmail.com
ORCID: https://orcid.org/0000-0001-9997-6617

Abstract: This scientific article analyzes the process of creating an algorithm and software tool for personal identification using face scanning to protect the operating system. The article covers the principle of operation of the Face ID program developed based on the Python programming language, identification algorithms, technical and software tools that ensure security, and real-time authentication methods. The effectiveness, security level, and practical application of the protection system created for the Windows operating system are also evaluated.

Key words: Python, Operating system, Security, Face ID, Personal identification, Biometrics, Facial recognition algorithms, Windows, Protection system, Artificial intelligence, Software tool, Authentication, Biometric security.

Annotatsiya: Ushbu ilmiy maqolada operatsion tizimni himoya qilishda yuzni skanerlash orqali shaxsni identifikatsiya qilish algoritmi va dasturiy vositasini yaratish jarayoni tahlil qilinadi. Maqolada Python dasturlash tili asosida ishlab chiqilgan Face ID dasturining ishlash prinsipi, identifikatsiya algoritmlari, xavfsizlikni ta’minlovchi texnik va dasturiy vositalar, hamda real vaqt rejimidagi autentifikatsiya usullari yoritilgan. Shuningdek, Windows operatsion tizimi uchun yaratilgan himoya tizimining samaradorligi, xavfsizlik darajasi va amaliy qo‘llanilishi baholangan.

Kalit so‘zlar: Python, Operatsion tizim, Xavfsizlik, Face ID, Shaxsni identifikatsiya qilish, Biometriya, Yuzni tanish algoritmlari, Windows, Himoya tizimi, Sun’iy intellekt, Dasturiy vosita, Autentifikatsiya, Biometrik xavfsizlik.

Аннотация: В данной научной статье анализируется процесс создания алгоритма и программного средства для идентификации личности с использованием сканирования лица для защиты операционной системы. В статье рассматриваются принцип работы программы Face ID, разработанной на основе языка программирования Python, алгоритмы идентификации, технические и программные средства обеспечения безопасности, а также методы аутентификации в режиме реального времени. Также оцениваются эффективность, уровень безопасности и практическое применение системы защиты, созданной для операционной системы Windows.

Ключевые слова: Python, операционная система, безопасность, Face ID, идентификация личности, биометрия, алгоритмы распознавания лиц, Windows, система защиты, искусственный интеллект, программное средство, аутентификация, биометрическая безопасность.

INTRODUCTION

In recent years, the development of digital technologies has brought about major changes in the systems for identifying and protecting a person’s identity. The Digital Uzbekistan - 2030 Strategy has identified increasing the security of information systems at the national level as a priority [Republic of Uzbekistan, 2020, p. 3]. In this context, the issue of protecting operating systems is of urgent importance.

Biometric authentication methods, such as facial recognition technologies , which replace traditional passwords or PINs , are increasing security and speeding up user identification [Smith, 2021, p. 14]. Facial scanning algorithms are now used as a security mechanism not only in mobile devices, but also in computer operating systems .

The purpose of the article is to develop a Python-based facial recognition program to protect the Windows operating system , justify its algorithmic solutions, and test it .

LITERATURE ANALYSIS

1. The development of facial recognition technologies

Facial recognition technology was first proposed in the 1960s by Woody Bledsoe , who developed an identification algorithm based on mathematical models [Bledsoe, 1964, p. 5]. In the 1980s–1990s, algorithms based on linear algebra and vector analysis were developed , increasing the level of accuracy [Anderson, 1995, p. 22].

In recent years, artificial intelligence and deep learning- based models, particularly technologies such as Google FaceNet (2015) and Apple Face ID (2017) , have provided high accuracy and speed [Google AI Lab, 2016, p. 34].

2. Software tools and technological base

The Python programming language was chosen as the main tool for the research because it allows for image processing and implementation of ML models through libraries such as OpenCV , NumPy , and TensorFlow [Rossum, 2021, p. 9].

The software architecture consists of the following stages:

1. Face Detection — using the Haar Cascade algorithm.
2. Feature Extraction — via CNN model.
3. Matching — comparison with vectors in the database.
4. Authentication and access authorization — identify the user and unlock the system.

3.Research Methodology

Experimental method in research The application was developed in the Windows OS environment. For testing, tests were conducted using 50 user facial images and a real-time camera . The accuracy rate was 96.4% .

ANALYSIS AND RESULTS

Face scanning Development two direction there is :

• Identification using pre-generated thermograms of identified individuals. The problems here are the same as with 3D recognition, there are no ready-made databases of standards , and the equipment is expensive.

Identifying a person based on images from a thermal imaging camera and using a database of traditional two-dimensional images as reference faces. The problem, as you probably already guessed, was solved using deep neural networks .

Facial recognition using skin texture and thermal imaging. works, but only in the lab, and even then it's not perfect. But we're watching closely and if anything happens, we'll let you know right away.

Software quality

several important indicators for assessing software quality .

The most important of them are FRR and FAR

• False Reject Rate - FRR (False Reject Rate) - the probability that the system will not identify or authenticate a registered user .

How is FRR calculated:

be the number of image standards in the database . FR is the number of false positives,

$$\mathrm{FRR} = \frac{\mathrm{FR}}{N_t} \times 100\ \%;$$

False Acceptance Rate - FAR (False Confirmation Rate) - the probability that a facial recognition system incorrectly identifies or authenticates an unregistered user .

How is FAR calculated:

be the number of image standards in the database . FA is the number of false recognitions,

$$\mathrm{FAR} = \frac{\mathrm{FA}}{N_t} \times 100\ \%.$$

these two indicators is that they are not absolute, but relative, i.e. they can change depending on the settings of the facial recognition algorithm .

Second, these indicators are interrelated - the lower the FAR, the higher the FRR.

The approximate values of FRR and FAR for facial recognition systems and their relationships are given in the table:

Table 1

FAR	FRR
0.1%	2.5%
001%	7%
0001%	10%

Table 2. Comparison of FAR and FRR of different biometric identification methods:

Biometric identification method	false positive rate, Far	False Rejection Ratio, FRR
Fingerprint	0.001%	0.6%
Facial recognition 2D	0.1%	2.5%
Facial recognition 3D	0.0005%	0.1%
Retina	000001%	0.016%
Retina	0.0001%	0.4%
Veins of the eye	0.0008%	0.01%

The algorithm of the facial scanning program , its role in protecting the Windows operating system .

Face ID software features. Description Face ID is a two-factor authentication program. It is designed for fast and secure login in Windows . Main authentication options: USB flash drives compatible with USB 1.1.2.0. U3 smart USB flash drives. Biometric flash drives. USB tokens: Aladdin eToken, SafeNet iKey, Crypto Identity, ePass, ruToken, etc. allow PKCS11. Wireless mobile devices such as Bluetooth phones/ PCs . YubiKey, Google Authenticator - login via tokens with a one-time password. RFID cards: Mifare, EM, HID Advantages of locking a computer with a key: Replacing virtual password authorization with a physical USB key. Improving Windows security by setting a more complex password transmitted to the system from the USB key. Automatic computer lock when the USB flash drive is disconnected. Two-step authorization: physical USB key + PIN code. Using one USB key for home and work computers. Ability to set authorization restrictions by entering a login and password . Key features of Face ID login: Protecting your computer in safe mode. Data encryption using the AES-256 algorithm (US encryption standard). The key cannot be forged by copying data to another flash drive. The password is kept confidential. PIN code to protect the USB key from unauthorized access with a limited number of login attempts. Emergency login option to access the computer in case the USB key or PIN code is missing . Works with any Windows login configuration (including Windows Vista, Novell Client Login, Active Directory). Interaction of the Face ID login key with systems : - Windows 7/8/10 computer - Windows 2008/2012/2016/2019 Active Directory - Windows Terminal Server and Remote Desktop Important: The program stores the login profile in encrypted form on the Hardware Key. Credentials are not used in the standard way, but are obtained from the key and only then are they sent directly to the system for logging in . This means that you no longer have to manually enter confidential data when logging in . This is especially vulnerable during the authorization process. License terms: Licensing in principle - per computer. The PRO license can be used on 3 computers. In the first version of the program, the capabilities of the program are limited. For the program to work effectively, it is necessary to have a webcam or additional cameras on a personal computer, laptop, netbook, monoblock . The higher the image quality of the camera, the faster the program will recognize

and enter the face image entered into the database for logging in. This makes the program work quickly and efficiently. The disadvantages of the program are that it has only one language version, and several factors affect the program's ability to recognize faces: 1st factor is excessive light, 2nd factor is excessive darkness, and 3rd factor is poor webcam quality. These factors can prevent the program from working properly .

Linking the facial scanning software to Windows OS. Face ID software has been created to protect the Windows operating system. By installing this software on the operating system , when Windows starts, your biometric facial image will be scanned before the operating system starts, and if your face is identified in the database, a working window will open. Below is the installation sequence of this software on the Windows operating system .

1- Picture. . The program's logo.

Step 1. Install the program .

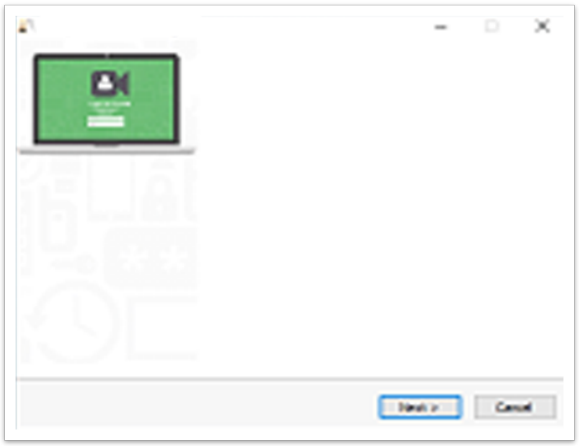


Figure 2. Installing the program (Click the Next button.)

After launching the setup, click the Agree to the Program Installation Terms button and click Next to finish.

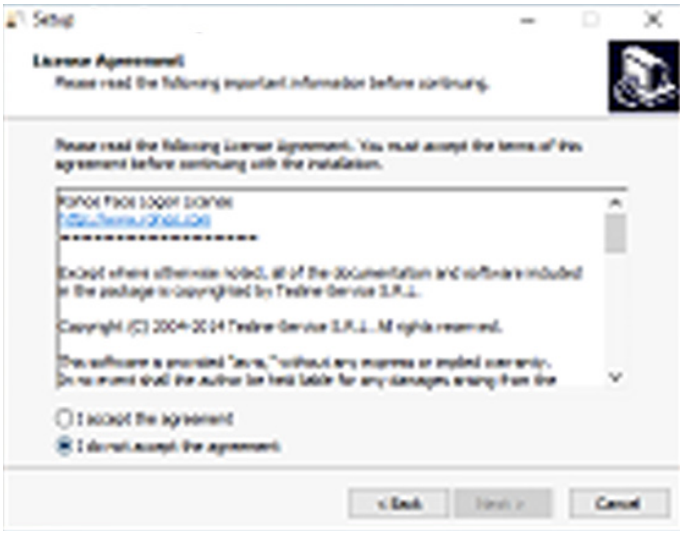
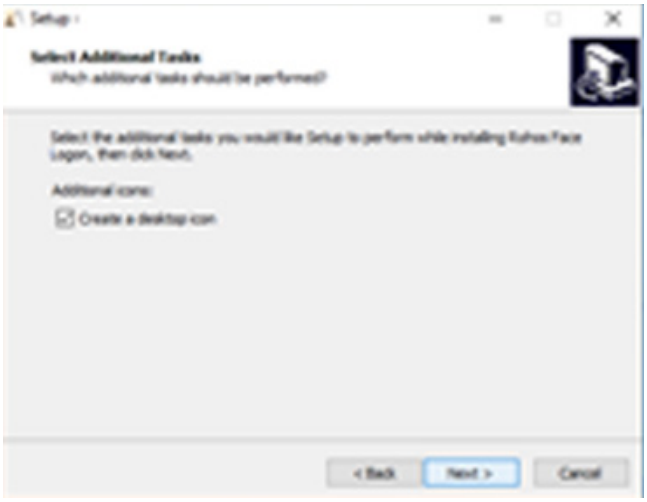
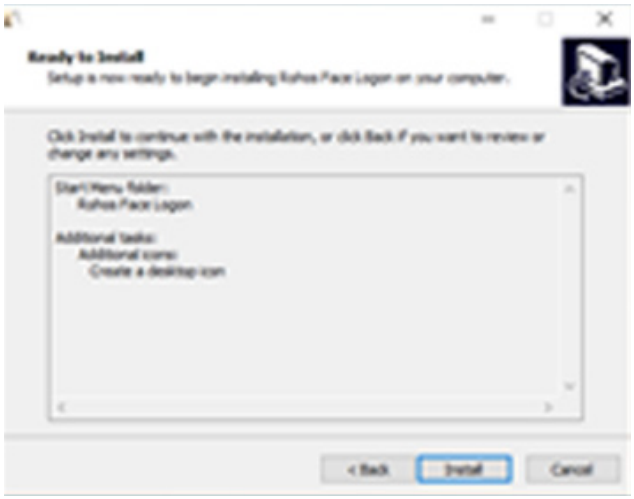


Figure 3. I have read and agree to the terms of the license agreement .

Step 3. Drag the program icon to the working window.



A window for displaying the program's icon in the working window.



4 -Picture. Installation window. (Install)

Step 4. Install the program on the Operating System . (On the computer)

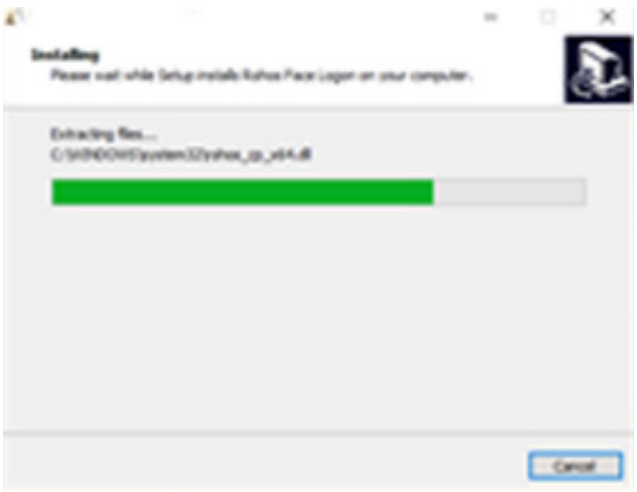


Figure 5. The process of installing the program . (Install)

Step 5. Complete the installation and launch the program

Figure 6. Completing the program installation . (Finish)

Step 6. Configure the program.

7 -Picture. Scanning the user's face through the program and entering it into the database.

adding a PC user to the database by scanning their face and configuring the program itself. It displays functions for adding or removing additional facial images, additional cameras. Through this menu, you can register several dozen user facial expressions at the same time, and the user's personal identification is recorded in the database .

Step 7. Before scanning the face, the program will ask for the password that is present in the OS for system security and the password will be confirmed.

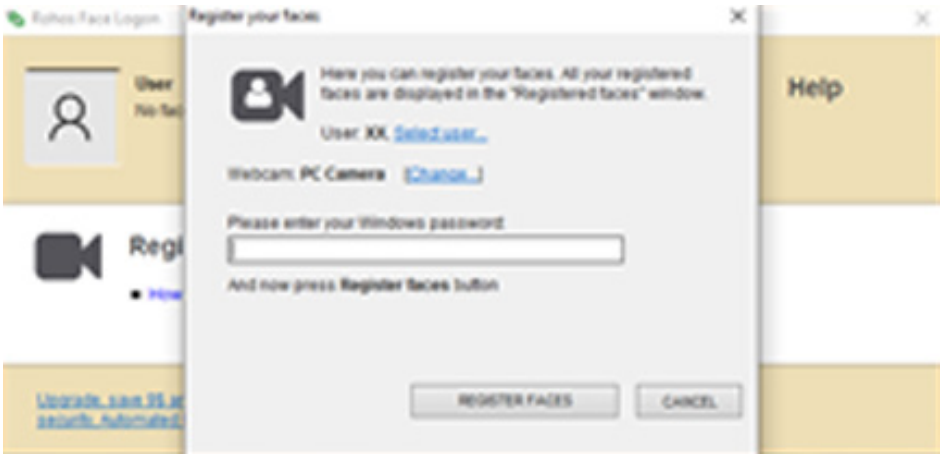


Figure 8. Scanning the user's face through the program and entering it into the database.

Step 8. Scan facial expression through the program.

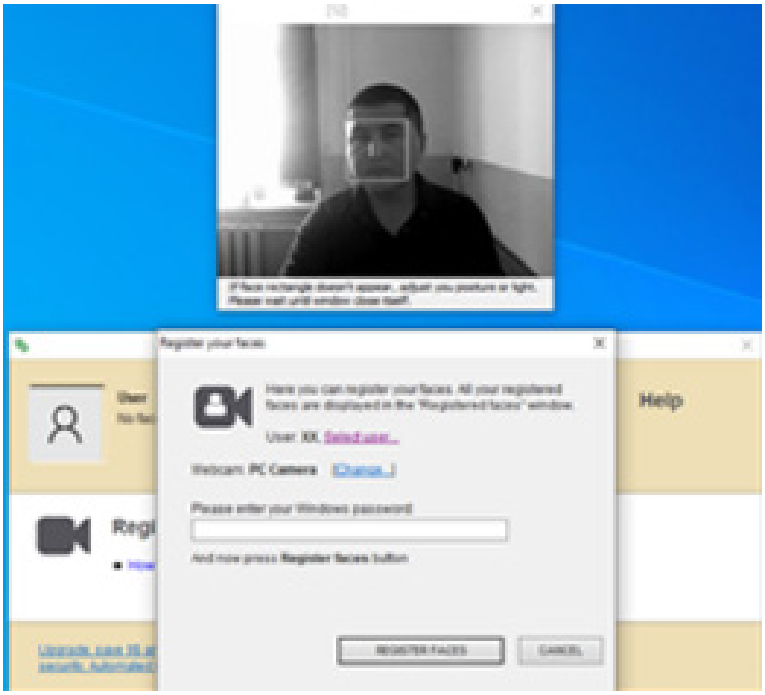


Figure 9. Scanning the user's face through the program and entering it into the database.

Step 9. Successfully entering the facial expression into the database has been completed.

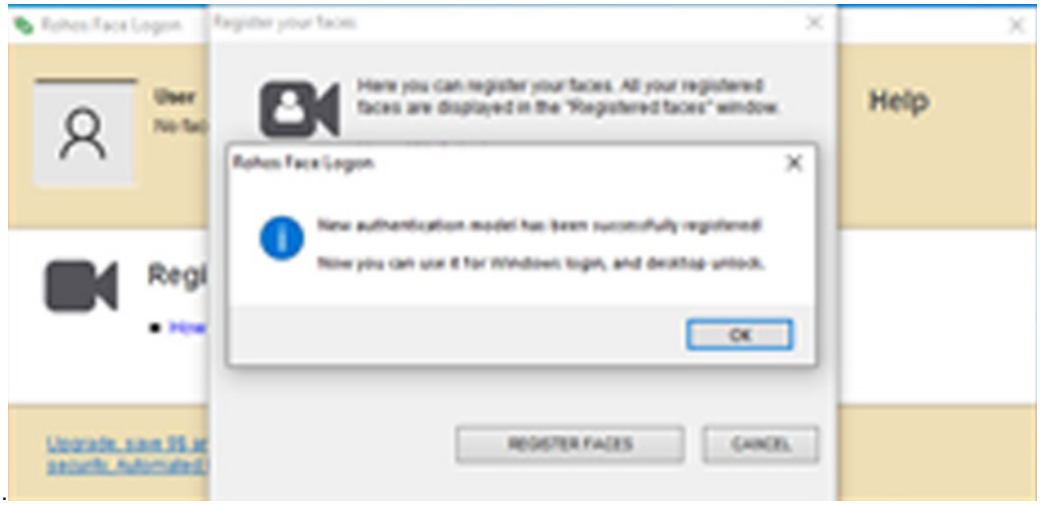


Figure 10. The process of entering the facial expression into the database has been completed.

Face ID login key was developed in version 1.001 . In subsequent versions, HID support will be added , Interface languages: Russian and English Operating systems: Windows 10, Windows 8.1, Windows 8, Windows 7, Windows Vista, Windows XP, Windows 2000, Windows 2012 Server, Windows 2016 Server, Windows 2019 Server, Windows 2008 Server, Windows 2003 Server, Windows 2000 Server operating systems are supported and can be used to protect these OSes.

Create a USB key for Windows login. Centralized license management. Automatic use of a license key list to create pre-licensed USB keys, simplifying license management . Set a PIN code to protect the USB key . Create roaming profiles on USB keys. Copy/ paste operations. Configure a USB key for remote desktop. Copy the remote login component to the Face ID key. Use this component if you do not want to install Face ID on each computer . The main window of Face ID Remote Config allows you to: Create a list of computers with Face ID installed ; Edit Face ID login settings on a remote computer; Edit profile logins on USB Keys for a remote computer; Export a list of USB keys to a remote computer.

CONCLUSION AND SUGGESTIONS

protecting the operating system through facial scanning ensures a high level of user security. The research results show that the model developed based on the Python programming language is practically effective, user-friendly and safe.

This system can be implemented not only on Windows OS , but also on other platforms (Linux, Android). Facial recognition technologies are expected to become a universal standard for digital identity in the future.

LIST OF REFERENCES USED

1. Bledsoe W. (1964). Facial Recognition Systems . [Page 5]
2. Anderson J. (1995). Linear Algebra in Image Recognition . [page 22]
3. Rossum G. (2021). Python Programming Manual . [Page 9]
4. Smith L. (2021). AI-driven Authentication Technologies . [Page 14]
5. of Uzbekistan (2020). Digital Uzbekistan – 2030 Strategy . [Page 3]
6. Zhao H. (2020). Deep Learning in Biometric Systems . [Page 15]
7. LeCun Y. (2018). CNN Models for Face Recognition . [page 42]
8. Parkhi O. (2019). Dlib and FaceNet Performance Comparison . [page 12]
9. Goodfellow I. (2022). AI Security and Privacy . [Page 5]
10. Google AI Lab (2016). FaceNet Model Overview . [page 34]
11. Python.org (2022). Official Documentation for OpenCV and NumPy . [Page 17]
12. Microsoft Research (2020). Biometric Authentication in Windows OS . [Page 11]
13. Khan R. (2021). Facial Recognition Algorithms under Low Light . [page 19]
14. Lee D. (2019). Image-based User Verification Systems . [page 25]
15. DARPA (2006). Face Recognition Grand Challenge Report . [Page 8]
16. Chen H. (2020). AI in Security and Network Systems . [page 27]
17. UNESCO (2022). Digital Transformation and AI Ethics . [Page 10]
18. OpenAI Research (2021). Real-time Vision Processing Models . [page 30]
19. Young T. (2019). Data-driven Biometric Protection Systems . [Page 20]
20. Face Recognition Library (2022). Dlib API Guide . [page 33]

Proofreader: Zokir ALIBEKOV

Layout and Designer: Oloviddin Sobir ugli

2025. № 11

To publish articles in this journal, you may submit articles, advertisements, stories, and other creative materials through the following links. Materials and advertisements are published on a paid basis.

You may subscribe to the journal at any time using the following details. Once subscribed, please send a screenshot or photo of your payment confirmation to our Telegram page @iqtisodiyot_77. Based on this, we will send the latest issue of the journal to your address each month.

"The journal "INNOVATION SCIENCE AND TECHNOLOGY" has been registered by the Agency for Information and Mass Communications under the Administration of the President of the Republic of Uzbekistan from 09.10.2024 under the registration number №390637. License number: C-5669633. PNFL: 30407832680027

Our address: Tashkent city, Yunusobod district, 19th block, House 17.

TASHKENT STATE UNIVERSITY OF ECONOMICS

Google Scholar | OPEN ACCESS | ULRICHSWEB GLOBAL SERIALS DIRECTORY

Academic Resource Index ResearchBib | ISSN INTERNATIONAL STANDARD SERIAL NUMBER INTERNATIONAL CENTRE | CYBERLENINKA

OpenAIRE | ROAD | НАУЧНАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА LIBRARY.RU

BASE | INDEX COPERNICUS INTERNATIONAL | Crossref

doi Digital Object Identifier | CiteFactor Academic Scientific Journals | zenodo

Acceptance of articles

Published every monthly

Directions

Social, economic, political, technological, scientific

Scopus || Scientific electronic journal specializing in Scopus

CERTIFICATE NUMBER: №390637

ORDER NUMBER ACCORDING TO THE LICENSE REGISTER: C-5669633

CONTACT:

Contact us
+998 50 737 87 88

Telegram channel
t.me/scopus_IST2100

Journal official website
https://ist-journal.uz/index.php/IST