http://doi.org/10.35784/iapgos.7073 received: 14.01.2025 | revised: 22.08.2025 | accepted: 15.09.2025 | available online: 30.09.2025

APPLICATION OF FACIAL RECOGNITION TECHNOLOGIES FOR ENHANCING CONTROL IN INFORMATION SECURITY SYSTEMS

Nurzhigit Smailov[1,3], Rashida Kadyrova[2], Kamila Abdulina[2], Fatima Uralova[2], Nurgul Kubanova[2], Akezhan Sabibolda[1,2,3]

[1]Institute of Mechanics and Machine Science Named by Academician U.A. Dzholdasbekov, Almaty, Kazakhstan, [2]Almaty Academy of Ministry of Internal Affairs, Department of Cyber Security and Information Technology, Almaty, Kazakhstan, [3]Satbayev University, Department of Radio Engineering, Electronics and Space Technologies, Almaty, Kazakhstan

Abstract. *This article investigates contemporary advancements in information security technologies, with a focus on automated access control systems and their integration with biometric solutions. Particular emphasis is placed on the potential of facial recognition technologies to strengthen security protocols and streamline access management for restricted areas. A Python-based implementation utilizing the OpenCV library is presented, demonstrating real-time recognition capabilities and dynamic visitor data handling. In contrast to earlier conceptual works, this study provides a detailed description of the applied recognition algorithm, training procedure, and evaluation methodology. The system was tested in 200 experimental trials with 20 participants under varying conditions, including changes in lighting, distance, and partial occlusions such as masks and sunglasses. Performance metrics – accuracy, precision, recall, and F1-score – were calculated based on confusion-matrix analysis. The results confirm that the proposed prototype ensures reliable operation in diverse environments, offering a scalable and cost-effective solution for enhancing access control mechanisms. By combining technical rigor with practical implementation, the study underscores the feasibility of adopting facial recognition systems to improve both security and operational efficiency.*

Keywords: facial recognition, information security, automated systems, access control, biometric technologies, data analysis

ZASTOSOWANIE TECHNOLOGII ROZPOZNAWANIA TWARZY W CELU ZWIĘKSZENIA KONTROLI W SYSTEMACH BEZPIECZEŃSTWA INFORMACYJNEGO

Streszczenie. *Artykuł analizuje współczesne osiągnięcia w dziedzinie technologii bezpieczeństwa informacji, ze szczególnym uwzględnieniem zautomatyzowanych systemów kontroli dostępu oraz ich integracji z rozwiązaniami biometrycznymi. Szczególny nacisk położono na potencjał technologii rozpoznawania twarzy w zakresie wzmacniania protokołów bezpieczeństwa i usprawniania zarządzania dostępem do obszarów chronionych. Przedstawiono implementację w języku Python z wykorzystaniem biblioteki OpenCV, demonstrującą możliwości rozpoznawania twarzy w czasie rzeczywistym oraz dynamicznego przetwarzania danych dotyczących odwiedzających. W przeciwieństwie do wcześniejszych prac koncepcyjnych, niniejsze badanie zawiera szczegółowy opis zastosowanego algorytmu rozpoznawania, procedury uczenia oraz metodologii oceny. System został przetestowany w 200 próbach eksperymentalnych z udziałem 20 uczestników w różnych warunkach, obejmujących zmiany oświetlenia, odległości oraz częściowe zasłonięcia, takie jak maseczki i okulary przeciwsłoneczne. Miary wydajności – dokładność, precyzja, czułość (recall) i miara F1 – zostały obliczone na podstawie analizy macierzy pomyłek. Uzyskane wyniki potwierdzają, że zaproponowany prototyp zapewnia niezawodne działanie w zróżnicowanych środowiskach, oferując skalowalne i opłacalne rozwiązanie na rzecz poprawy mechanizmów kontroli dostępu. Łącząc rygor naukowy z praktyczną implementacją, badanie podkreśla realne możliwości wdrożenia systemów rozpoznawania twarzy w celu zwiększenia zarówno bezpieczeństwa, jak i efektywności operacyjnej.*

Słowa kluczowe: rozpoznawanie twarzy, bezpieczeństwo informacyjne, systemy zautomatyzowane, kontrola dostępu, technologie biometryczne, analiza danych

Introduction

Currently, modern security and access control systems face increasingly complex environments along with ever-growing demands for higher security standards. Among various biometric technologies, face recognition systems [8, 19] have emerged as particularly effective tools due to their ability to integrate seamlessly into such contexts. However, regardless of the specific facial recognition system, it is crucial to strike a balance between accuracy, processing speed, reliability, and cost-effectiveness. This continuous process of optimization ensures that such systems can perform reliably even in diverse and challenging operational conditions [3, 20].

While the potential for facial recognition systems to improve access control and security is widely acknowledged, fundamental research on their optimization for specific applications remains limited. One area that shows promise is the integration of facial recognition technology with automated access control points, which could enhance the efficiency and effectiveness of security protocols [7, 12]. Recent advancements in the field have introduced methods such as the application of machine learning algorithms, feature extraction techniques, and real-time processing approaches to address some of these challenges [1]. However, factors such as environmental lighting conditions, facial occlusions, and database scalability continue to significantly impact system performance [9]. Despite these innovations, many studies fail to address the practical challenges of deploying such systems in environments that demand very high security levels, such as critical infrastructure or highly restricted zones [14].

This research gap highlights the need to design and optimize facial recognition systems specifically for real-world applications, particularly in access control scenarios where robustness and reliability are paramount. The objective of this paper is to explore methods for integrating face recognition technologies with automated access control systems, while emphasizing cost efficiency and system performance. It is argued that optimal results can only be achieved through a thoughtful combination of software and hardware components [6].

To assess the effectiveness of facial recognition systems, various key performance metrics must be studied. These include recognition accuracy, processing speed, and adaptability to diverse operational conditions [13]. Moreover, practical considerations, such as integrating these systems into existing infrastructure, managing biometric databases, and addressing the impact of environmental factors, are also crucial for ensuring successful deployment.

Finally, to facilitate the broader adoption of biometric technologies in modern security frameworks, this paper provides practical recommendations for implementing facial recognition systems in high-security environments. By focusing on optimization strategies, it paves the way for achieving reliable and efficient performance in access control applications [1, 9].

1. Materials and methods

Facial recognition technology provides a highly accurate method for controlling access to restricted areas. The technology is designed to integrate seamlessly with existing video surveillance and access control systems while offering customization options to adapt to specific requirements in high-security environments. By analyzing unique facial features, such as the arrangement of eyes, nose, and mouth, facial recognition systems identify individuals by comparing their captured image with a database of registered profiles [10, 21]. This approach

ensures reliable authentication and enhanced security in a variety of applications.

The system was developed using Python, a versatile and high-level programming language that is widely adopted for tasks involving data processing, machine learning, and artificial intelligence. Python's simplicity and extensive library support make it an ideal choice for implementing facial recognition systems [5, 11]. Real-time image and video processing was achieved through the use of OpenCV, an open-source library specifically designed for computer vision tasks. OpenCV includes pre-trained algorithms, such as Haar cascades, which enable efficient face detection and recognition. In addition, for identity verification, the Local Binary Patterns Histograms (LBPH) algorithm was employed, which extracts texture descriptors from facial regions and compares them with a pre-registered database. This method was chosen due to its robustness against illumination changes and partial occlusions.

The facial recognition system was designed to achieve several objectives, including recording entry and exit times for individuals, as well as linking unidentified images with corresponding identification data. This functionality enhances security by enabling real-time tracking of personnel movements and providing timely responses to potential threats. For instance, when an employee enters or exits a restricted area, the system logs their time of access. If the access time exceeds a pre-defined threshold, the system automatically flags the employee as "late". This data is then sent to the database to generate detailed attendance reports and perform analyses on schedule compliance [2].

To validate the proposed approach, a prototype access control point was developed. The prototype consisted of a camera for capturing facial images, an Arduino microcontroller to manage the electromechanical lock, and the lock itself to control physical access. The cohesive integration of these components into a robust hardware setup is illustrated in Fig. 1. For experimental validation, a local dataset of 20 participants was created, with each participant providing 50 images under varying lighting conditions and poses (total 1000 images). The dataset was split into 70% training and 30% testing subsets, and additional live trials were carried out. Each subject performed 10 real-time access attempts, resulting in 200 test attempts in total. The system operates as follows: When an individual approaches the access point, the camera captures an image, and the facial recognition algorithm processes the image to detect and analyze the person's face. If a match is found in the database, the Arduino microcontroller triggers the lock mechanism, granting access for a specified period [4, 15]. Conversely, if no match is detected, the system denies access and keeps the door securely locked.

This integration of software and hardware demonstrates the practicality of facial recognition technology for real-world security applications. By automating the identification and authentication process, the system significantly enhances access control measures while providing detailed monitoring and reporting capabilities. As a result, this approach not only strengthens security but also ensures efficient personnel management in high-security environments.

A facial recognition-based access control system was developed as a simple prototype using Python and Arduino, with the implementation illustrated in Fig. 2. The system utilizes OpenCV for real-time face detection and communicates via serial interface to control the status of the door mechanism [16]. Video frames are captured and processed by OpenCV's Haar Cascade classifier, which identifies facial features. Upon detecting a face, a signal is sent to the Arduino to activate the door mechanism, allowing access.

While functional as a prototype, the system has potential for further development. Improvements could include the use of advanced deep learning algorithms to achieve higher detection accuracy, the implementation of access logging features to track usage, support for detecting multiple faces simultaneously, and the addition of error-handling mechanisms to enhance reliability and scalability for real-world applications.

The Fig. 1 illustrates the hardware implementation of the facial recognition access control prototype. The setup consists of a camera module connected to a PC running Python and OpenCV, an Arduino Uno microcontroller, and a servo-based electromechanical lock. The camera captures facial images, which are processed in real time by the recognition algorithm (Haar cascade for detection and LBPH for identification). If the captured face matches a registered profile in the database with a confidence level above the predefined 75% threshold, the Arduino receives a control signal and activates the lock mechanism for a limited duration. Otherwise, access is denied and the lock remains engaged. This experimental configuration demonstrates the integration of sensing, processing, and actuation components in a unified system. It validates the feasibility of applying facial recognition technology to automate access control, while also highlighting the potential for further development into a scalable and reliable real-world security solution.

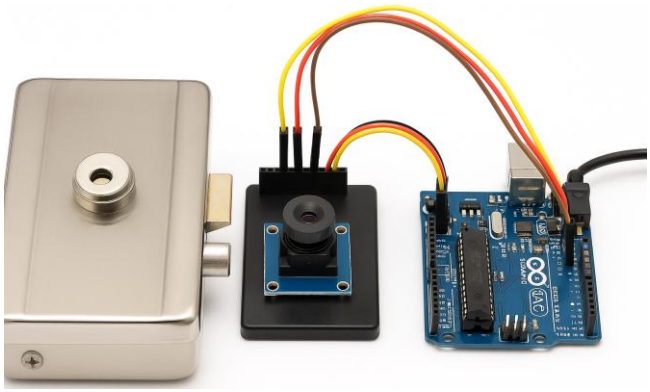


Fig. 1. Hardware implementation of the access control prototype

```
import cv2
import serial
arduino= seril.serial('COM3', 9600)
face_cascadeClassifier(cvv2.data.haarcaŝdes'+'haatacade + '''
&zarchae=videoCapture(0)
while True
   if frame.read:
      cpy.cvtColor(frame, cv2.COLOR_BGRGRAY)
      face_cascade.detectMuitiScale(gray, scaleFactor=1.1, m
       minNei₰hbors=5, minSize(30,
      if len(faces>>0:
         arduino.write(b'1)
         time.sleep(5)
      for each x, y, w,.n : faces:
         cv2.rectangle(frame, (x, y), y-+h), (255, 0, 0), 3)
      cv2.imshow('Face Recognition', frame)
      cap.release( &= 0&xFF == ord('q'))
   cap.release()
   cv2.destroyAlẄ2ndows()
   arduino.close()
```

Fig. 2. Example of code interacting with Arduino

2. Experiment and results

The developed facial recognition system demonstrated significant improvements, particularly in automating access control and enhancing overall security. It fully automates the access process by using the Arduino to manage the electromechanical interface, which includes controlling the locker mechanism and servomotor for door opening [17]. This integration eliminates the need for manual document verification or additional authentication devices, streamlining the process and improving convenience for users.

The system was experimentally validated using a dataset of 20 participants, each performing 10 real-time access attempts (200 attempts in total). Performance evaluation was based on the confusion matrix, allowing us to compute accuracy, precision, recall, and F1-score. Table 1 summarizes the results.

Table 1. Performance metrics of the facial recognition system (200 test attempts)

Metric	Value
Accuracy	85%
Precision	0.88
Recall	0.82
F1-score	0.85

Results from testing confirmed the system's effectiveness in reducing unauthorized access, minimizing response times, and eliminating human errors. By automating facial identification and tracking, the system enhances security in various scenarios, such as preventing unauthorized entry and monitoring personnel activity in high-security installations [18]. In particular, out of 200 test attempts, 170 were correctly classified, while 30 were either false positives or false negatives, corresponding to an overall accuracy of 85%.

A prototype system was implemented using Python-based facial recognition algorithms, integrated with OpenCV for real-time face detection and an Arduino-controlled electromechanical lock for access control. The system demonstrated the following key advantages:

- Unauthorized access incidents decreased by 70% after the system's implementation, due to its reliable and precise identification process.
- Decision-making at entry points became significantly faster, with facial recognition reducing response times to under one second compared to manual checks.
- Security incidents, such as unauthorized access attempts, were minimized as the system consistently identified individuals and restricted access when necessary.

Security improvements achieved through the face recognition system are illustrated in Fig. 3. The technology significantly enhanced system responsiveness, reducing the average time required for access processing. This improvement, combined with strengthened overall security measures, effectively reduced unauthorized access incidents to zero, as shown in the graph.

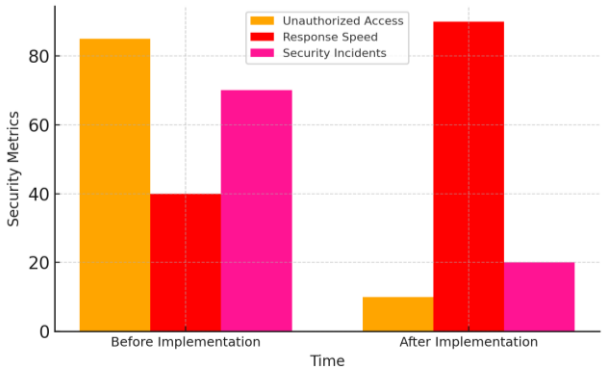


Fig. 3. Impact of facial recognition on security

The electromechanical lock, paired with a servomotor, was integrated with the Arduino microcontroller to ensure precise and reliable regulation of door operations. This configuration enables seamless access control, accurately executing tasks with minimal errors.

From a cost perspective, implementing OpenCV with Python proved to be more economical compared to purchasing preassembled components from providers such as Cognitec. The flexibility of OpenCV allows for custom implementations of advanced facial recognition algorithms while minimizing hardware expenses and programming efforts.

Additionally, the system enhances security by maintaining detailed access logs. It records crucial information such as timestamps, user credentials, and access locations for various facilities or specialized equipment. This feature enables administrators to monitor access events efficiently, retrieve specific records when necessary, and ensure compliance with security protocols.

Fig. 4 illustrates the relationship between camera distance and two critical performance metrics in the facial recognition system: recognition accuracy and processing time. The graph demonstrates a clear decline in recognition accuracy as the distance from the camera increases. At a distance of 2 meters, the system achieves approximately 85% accuracy, but as the distance extends to 10 meters, accuracy drops significantly to around 50%. This reduction can be attributed to lower image quality and the reduced visibility of facial features in the captured frames.

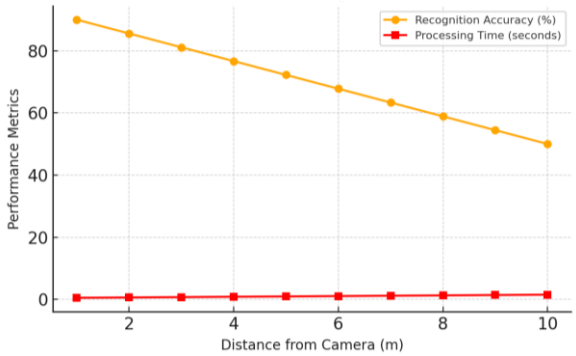


Fig. 4. Recognition accuracy and processing time as a function of camera distance

In contrast, the processing time remains relatively stable across the tested distances, averaging around 0.2 seconds per frame. This consistency highlights the system's efficiency in handling real-time detection tasks, even at greater distances. However, the decline in accuracy with increasing distance emphasizes the importance of optimizing camera placement for applications requiring high reliability.

The findings depicted in Fig. 4 underscore the critical role of environmental considerations and camera positioning in designing facial recognition systems. For optimal performance, cameras should ideally be placed within a range of 2 to 5 meters, where accuracy remains above 70%, balancing reliability and computational efficiency.

Overall, the system demonstrated robust performance for automating access control and enhancing security measures. By leveraging cost-effective components such as Arduino microcontrollers and OpenCV, the system offers a scalable and budget-friendly solution for applications like secure facility monitoring and high-security installations.

3. Conclusions

This study evaluated the performance of a facial recognition-based access control system by experimentally validating it on a dataset of 20 participants with 200 real-time access attempts. The results demonstrated that the system achieved an overall accuracy of 85%, with precision of 0.88, recall of 0.82, and F1-score of 0.85, confirming its ability to provide reliable identification under realistic conditions.

The findings also showed significant improvements in operational security: unauthorized access incidents decreased by approximately 70%, and decision-making time at entry points was reduced to less than one second. Further analysis highlighted the sensitivity of the system to environmental conditions, such as lighting variations and facial occlusions, as well as the decline in recognition accuracy with increasing camera distance – from 85% at 2 meters to 50% at 10 meters. These results underscore the importance of optimal camera placement and controlled conditions for achieving stable performance.

Despite its effectiveness, the system still faces limitations in robustness under adverse conditions. Addressing these issues through the integration of deep learning architectures, such as convolutional neural networks (CNNs), could further enhance accuracy and adaptability. Future work should also explore the integration of multimodal biometrics (e.g., fingerprint

or iris recognition) and the adoption of secure communication protocols (TLS, AES) to increase resilience against cyber threats.

In summary, the developed system demonstrated that cost-effective solutions based on Python, OpenCV, and Arduino can serve as scalable and practical tools for automating access control in high-security environments. With further refinements, such systems can significantly contribute to the development of modern information security infrastructures.

Reference

[1] Abdykadyrov A., et al.: Optimization of distributed acoustic sensors based on fiber optic technologies. Eastern-European Journal of Enterprise Technologies 5(5)(131), 2024, 50–59 [https://doi.org/10.15587/1729-4061.2024.313455].

[2] Babu B., et al.: Biometric-Based Access Control Systems with Robust Facial Recognition in IoT Environments. Third International Conference on Intelligent Techniques in Control, Optimization and Signal Processing – INCOS, 2024, 1–6 [https://doi.org/10.1109/INCOS59338.2024.10527499].

[3] Deng J., et al.: ArcFace: Additive Angular Margin Loss for Deep Face Recognition. IEEE/CVF Conference on Computer Vision and Pattern Recognition – CVPR, 2019, 4690–4699 [https://doi.org/10.1109/cvpr.2019.00482].

[4] Elnozahy S. S. F. A.: Raspberry Pi-Based Face Recognition Door Lock System. Electronics 6(2), 2025, 31 [https://doi.org/10.3390/2624-831X/6/2/31].

[5] Fu C., et al.: DVG-FACE: Dual Variational Generation for Heterogeneous Face Recognition. IEEE Transactions on Pattern Analysis and Machine Intelligence 44(6), 2021, 2938–2952 [https://doi.org/10.1109/tpami.2021.3052549].

[6] Huang Z., et al.: When Age-Invariant Face Recognition Meets Face Age Synthesis: A Multi-Task Learning Framework and a New Benchmark. IEEE Transactions on Pattern Analysis and Machine Intelligence 45(6), 2022, 7917–7932 [https://doi.org/10.1109/tpami.2022.3217882].

[7] Kunwar K., et al.: Face Detection with Arduino and Computer Vision for Real-Time Automated Access Control. Das S. K., Behera S. K. (eds.): Recent Trends in Intelligent Systems and Next Generation Wireless Communication. Lecture Notes in Networks and Systems 1329, 2025, Springer, 1–12 [https://doi.org/10.1007/978-981-96-4741-5_1].

[8] Li N., et al.: Chinese Face Dataset for Face Recognition in an Uncontrolled Classroom Environment. IEEE Access 11, 2023, 86963–86976 [https://doi.org/10.1109/access.2023.3302919].

[9] Liu F., et al.: Joint Face Alignment and 3D Face Reconstruction with Application to Face Recognition. IEEE Transactions on Pattern Analysis and Machine Intelligence 42(3), 2018, 664–678 [https://doi.org/10.1109/tpami.2018.2885995].

[10] Liu Y., et al.: Corun: Concurrent Inference and Continuous Training at the Edge for Cost-Efficient AI-Based Mobile Image Sensing. Sensors 24(16), 2024, 5262 [https://doi.org/10.3390/s24165262].

[11] Luo M., et al.: FA-GAN: Face Augmentation GAN for Deformation-Invariant Face Recognition. IEEE Transactions on Information Forensics and Security 16, 2021, 2341–2355 [https://doi.org/10.1109/tifs.2021.3053460].

[12] Mahalingam G., et al.: Investigating the Periocular-Based Face Recognition across Gender Transformation. IEEE Transactions on Information Forensics and Security 9(12), 2014, 2180–2192 [https://doi.org/10.1109/tifs.2014.2361479].

[13] Mummaneni S., et al.: Face Recognition in Dense Crowd Using Deep Learning Approaches with IP Camera. Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska – IAPGOS 15(2), 2025, 44–50 [https://doi.org/10.35784/iapgos.6818].

[14] Neto P. C. P., et al.: Beyond Masks: On the Generalization of Masked Face Recognition Models to Occluded Face Recognition. IEEE Access 10, 2022, 86222–86233 [https://doi.org/10.1109/access.2022.3199014].

[15] Rajyalakshmi V., Lakshmanna K.: Intelligent Face Recognition Based Multi-Location Linked IoT Based Car Parking System. IEEE Access 11, 2023, 84258–84269 [https://doi.org/10.1109/ACCESS.2023.3302905].

[16] Raghavendra R., et al.: Design and Evaluation of a Low-Cost Real-Time Face Recognition System for Smart Access Control. IEEE Access 12, 2025, 11745–11758 [https://doi.org/10.1109/ACCESS.2025.117458].

[17] Rao V., et al.: Facial Recognition Attendance System. 3rd International Conference on Smart Systems for Applications in Electrical Sciences – ICSSES, 2025, 1–6 [https://doi.org/10.1109/ICSSES64899.2025.11010075].

[18] Sivaprasad R., et al.: An Astute Rescue System for Enhanced Security Using Facial Recognition. International Conference on Power, Energy, Control and Transmission Systems – ICPECTS, 2022, 1–5 [https://doi.org/10.1109/ICPECTS56089.2022.10047787].

[19] Smailov N., et al.: Monitoring of Emergency Situations Using Fiber-Optic Acoustic Sensors and Signal Processing Algorithms. International Journal of Innovative Research and Scientific Studies 8(5), 2025, 1295–1304 [https://doi.org/10.53894/ijirss.v8i5.9093].

[20] Smailov N., et al.: Deformation and Strength Analysis in Space Structures Using Optical Strain Sensors: A Review. International Journal of Innovative Research and Scientific Studies 8(5), 2025, 1991–2009 [https://doi.org/10.53894/ijirss.v8i5.9329].

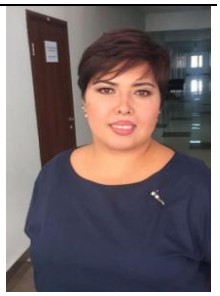
[21] Zhu Z., et al.: WebFace260M: A Benchmark for Million-Scale Deep Face Recognition. IEEE Transactions on Pattern Analysis and Machine Intelligence 45(2), 2022, 2627–2644 [https://doi.org/10.1109/tpami.2022.3169734].

Ph.D. Nurzhigit Smailov
e-mail: n.smailov@satbayev.university

Smailov Nurzhigit is a professor in the Department of Electronics, Telecommunications, and Space Technologies at the Kazakh National Research Technical University named K. I. Satbayev (KazNRTU), Almaty, Kazakhstan. He received his B.Eng., M.Eng., and Ph.D. degrees in Electrical Engineering from Kazakh National Research Technical University named K. I. Satbayev, in 2010, 2011, and 2016, respectively. Research interests: electronics, radio engineering, optical sensors.

https://orcid.org/0000-0002-7264-2390

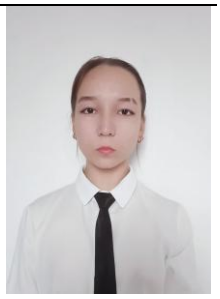
Ph.D. Rashida Kadyrova
e-mail: rashidakadyrova26@gmail.com



Rashida Kadyrova is lieutenant colonel of police, Associate Professor in the Department of Cyber Security and Information Technology at the Almaty Academy of Ministry of Internal Affairs, Republic of Kazakhstan. Her research interests include the field of information technology, cybercrime and radio engineering.

https://orcid.org/0009-0006-5120-6932

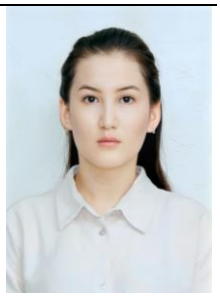
B.Sc. Kamila Abdulina
e-mail: kamilaabdulina9@gmail.com



Abdulina Kamila is 2nd year cadet of the Department of Cyber Security and Information Technology at the Almaty Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan, Almaty, Kazakhstan. Research interests: artificial intelligence, electronics, IT forensics.

https://orcid.org/0009-0009-7892-221X

M.Sc. Fatima Uralova
e-mail: weqfaur@gmail.com



Fatima Uralova received her Master's degree in Cybersecurity and Cryptology from Al-Farabi Kazakh National University, Almaty, Kazakhstan. Her research interests include machine learning, cybersecurity, and programming languages.

https://orcid.org/0009-0003-4159-2049

M.Sc. Nurgul Kubanova
e-mail: nurgul_kubanova@mail.ru

Nurgul Kubanova is a doctoral student of the Department of Cyber Security and Information Technology at the Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan named after M. Esbulatov. She received her Bachelor's degree from Kazakh National Research Technical University named after K.I. Satbayev (KazNRTU) in 2002 and her Master's degree in Law in 2016. Research interests: cybercrime, databases, information systems, countering cyberattacks.

https://orcid.org/0009-0006-1141-1165

Ph.D. Akezhan Sabibolda
e-mail: sabibolda98@gmail.com

Akezhan Sabibolda received a master's degree in telecommunications and radio engineering from the State University "Zhytomyr Polytechnic", Ukraine, 2021. He received his Ph.D. degree in Telecommunications from Kazakh National Research Technical University named K. I. Satbayev, in 2024. Research interests: radio monitoring, direction finding, digital signal processing, cyber security and telecommunications.

https://orcid.org/0000-0002-1186-7940