ТЕХНИЧЕСКИЕ НАУКИ
И ТЕХНОЛОГИИ

АҚПАРАТТЫҚ ЖҮЙЕЛЕР
ИНФОРМАЦИОННЫЕ СИСТЕМЫ
INFORMATION SYSTEMS

DOI 10.51885/1561-4212_2023_4_249
IRSTI 20.20.53.

B. Kopzhasarov[1], A.K. Koshekov[2], S. Adikanova[1], M. Bazarova[1], A. Kadyrova[1], M. Rakysheva[3], A. Bugubayeva[4]
[1]Sarsen Amanzholov East Kazakhstan university, Ust-Kamenogorsk, Kazakhstan
E-mail: atzhal@yande.ru
E-mail: ersal_7882@mail.ru
E-mail: madina_vkgtu@mail.ru
E-mail: kas-kas-50@mail.ru
[2]Academy of Civil Aviation, Almaty, Kazakhstan
*E-mail: abai_koshekov@mail.ru**
[3]East Kazakhstan Technical University. D. Serikbaeva, Kazakhstan
E-mail: Rakysheva.madina@gmail.com
[4]Karaganda University of Kazpotrebsoyuz, Karaganda, Kazakhstan
E-mail: alina_bugubayeva@mail.ru

DEVELOPMENT OF AN ACCESS CONTROL AND MANAGEMENT SYSTEM USING A SOFTWARE APPLICATION

БАҒДАРЛАМАЛЫҚ ҚОСЫМШАНЫ ПАЙДАЛАНА ОТЫРЫП, ҚОЛ ЖЕТКІЗУДІ БАСҚАРУ ЖӘНЕ БАСҚАРУ ЖҮЙЕСІН ӘЗІРЛЕУ

РАЗРАБОТКИ СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ С ИСПОЛЬЗОВАНИЕМ ПРОГРАММНОГО ПРИЛОЖЕНИЯ

Annotation*. The administration of educational institutions has several multi-storey buildings, in which it is necessary to carry out a set of technical and organizational measures to control visitors by security personnel. The lack of the possibility of registering students does not allow for the identification of their identity, which makes it difficult to investigate incidents of discipline violations and location. Registration of passport data of visitors with a small number of supervisory personnel is not suitable for the business processes of educational institutions. Measures to ensure the safety of visitors are carried out in educational institutions by selective control of visitors by security personnel, installation of remote control systems, video surveillance equipment.*

Functional modeling methods and programming were used to implement the identification and authentication method in the access system. The use of mobile devices, cards with a chip with a set of identification data implements the technology of their transmission, automating the access regime in educational institutions.

The materials are compiled based on the results of research and development of an access control and management system using a MySQL, Python based software application. The article presents an analysis of the technology for developing a control and access system developed on the basis of Proximity. An experimental test of the software application obtained during the study was carried out, which implemented technologies for organizing communication with network devices, automatic detection of mobile devices in the database, user recognition by identification code.

The software application interacts with other applications and chips, exchanges information, unidirectional communication with data stored on the server. A software application using PHP and MySQL database for student access control based on mobile devices can be used to determine the location of students who have passed the control.

Keywords: *control and access system, identification code, chip cards, database, PHP, mobile device, MySQL,* *location, identification code (ID).*

Аңдатпа. *Білім беру мекемелерінің әкімшілігінде бірнеше көп қабатты ғимараттар бар, онда күзет қызметінің қызметкерлері келушілерді бақылаудың техникалық және ұйымдастырушылық шараларының кешенін жүргізуі керек. Білім алушыларды тіркеу мүмкіндігінің болмауы жеке басын сәйкестендіру рәсімін жүргізуге мүмкіндік бермейді, бұл тәртіпті бұзу оқиғалары мен орналасқан жерін тергеуді қиындатады. Бақылаушы персоналдың аз санымен келушілердің төлқұжат деректерін тіркеу Білім беру мекемелерінің бизнес-процестеріне сәйкес келмейді. Келушілердің қауіпсіздігін қамтамасыз ету жөніндегі шаралар күзет қызметкерлері келушілерді іріктеп бақылау, пульттік күзет жүйелерін, бейнебақылау құралдарын орнату арқылы білім беру мекемелерінде жүргізіледі.*

Функционалды модельдеу әдістері, қол жеткізу жүйесінде сәйкестендіру және аутентификация әдісін жүзеге асыру үшін бағдарламалау қолданылады. Мобильді құрылғыларды, сәйкестендіру деректері жиынтығы бар чипі бар карточкаларды пайдалану оларды беру технологиясын жүзеге асырады, білім беру мекемелерінде өткізу режимін автоматтандырады.

Материалдар MySQL, Python негізіндегі бағдарламалық қосымшаны пайдалана отырып, қол жеткізуді бақылау және басқару жүйесін зерттеу және әзірлеу қорытындылары бойынша құрастырылған. Мақалада proximity негізінде жасалған бақылау және қол жеткізу жүйесін әзірлеу технологиясының талдауы берілген. Зерттеу барысында алынған бағдарламалық қосымшаға эксперименттік тексеру жүргізілді, онда желілік құрылғылармен байланысты ұйымдастыру, дерекқорға мобильді құрылғыларды автоматты түрде анықтау, пайдаланушыларды сәйкестендіру коды бойынша тану технологиялары іске асырылды.

Бағдарламалық қосымшада басқа қосымшалармен және чиптермен өзара іс-қимыл, ақпарат алмасу, серверде сақталған деректермен бір бағытты байланыс жүзеге асырылады. PHP және MySQL мәліметтер базасын қолдана отырып, мобильді құрылғыларға негізделген білім алушылардың қол жетімділігін бақылау бағдарламалық қосымшасы бақылаудан өткен білім алушылардың орналасқан жерін анықтау үшін пайдаланылуы мүмкін.

Түйін сөздер: *басқару және қол жеткізу жүйесі, сәйкестендіру коды, Чип карталары, дерекқор, PHP, мобильді құрылғы, MySQL, орналасқан жері, сәйкестендіру коды (ID).*

Аннотация. *Администрация образовательных учреждений имеет несколько многоэтажных корпусов, в которых надо проводить комплекс технических и организационных мер контроля посетителей сотрудниками службы охраны. Отсутствие возможности регистрации обучающихся не позволяют проводить процедуру идентификации] личности, это затрудняет расследование инцидентов нарушения дисциплины и местонахождения. Регистрация паспортных данных посетителей при небольшой численности контролирующего персонала не подходит бизнес-процессам образовательных учреждений. Меры по обеспечению безопасности посетителей осуществляются в образовательных учреждениях путем установки дистанционных систем безопасности, оборудования видеонаблюдения и выборочного контроля сотрудников службы безопасности, входящих в помещение.*

Использованы методы функционального моделирования, программирование для реализации способа идентификации и аутентификации в системе доступа. Использование мобильных устройств, карточек с чипом с набором идентификационных данных осуществляет технологию их передачи, автоматизируя пропускной режим в образовательных учреждениях.

Материалы составлены по итогам исследования и разработки системы контроля и управления доступом с использованием программного приложения на основе Python, MySQL. В статье представлен анализ технологии разработки системы контроля и доступа, разработанной на базе Proximity. Проведена экспериментальная проверка программного приложения, полученных в ходе исследования, в котором реализована технологии организации связи с сетевыми устройствами, автоматического определения мобильных устройств в базу данных, распознавания пользователей по идентификационному коду.

В программном приложении осуществлены взаимодействие с другими приложениями и микросхемами, обмен информацией, однонаправленная связь с данными, хранящимися на сервере. Программное приложение с помощью PHP и базы данных MySQL по контролю доступа обучающихся на основе мобильных устройств может быть использована для определения местоположения обучающихся, прошедших контроль.

Ключевые слова: *система контроля и доступа, идентификационный код, карты с чипом, база данных, PHP, мобильное устройство, MySQL, местонахождение, идентификационный код (ID).*

Introduction. Many objects of transportation infrastructure and presence of public places are equipped with citizen safety measures. This achieves through access control. Educational institutions may be included in the list of objects, which are not subject to mandatory police protection. The management of such facilities implements a range of technical and organizational measures to ensure the safety of visitors. Security personnel monitor visitors, and access points use surveillance equipment, metal detectors, and remote control alarm systems [1]. However, since there is no user registration system, the procedure for identifying a visitor is not possible. The administration of an educational institution ensures the safety of visitors and takes measures to ensure their safety during visits. We have made some changes, such as installing a turnstile that operates with a software application [1, 2].

Registration passport data of visitors is incompatible with the business processes of educational institutions. Registering all of incoming visitors is challenging with a small number of employees. Security measures for visitors include selective control by security personnel, the installation of remote protection systems, and the provision of services to educational institutions using surveillance measures [3]. Constant movement of students and the absence of opportunities to register visitors make identification procedures impossible. There is a threat of unauthorized access to the facilities. It is difficult to register participants or determine their location in an educational institution or student dormitory because student information cannot be identified. The task is to study approaches and methods that can organize the accounting of student flows without harming the organization's business processes [4].

Literature review. The issue of personal identification has many solutions. This problem is described in the works of B. Schneier, N. Skandhakumar, A. Dmitrienko, J. Brainard, S. Schechter, S. Egelman, R.W. Reeder, A.A. Malkova, V.V. Volkonsky, A.G. Sabanov, and V.A. Tikhonov [1, 5]. The development of technical means of protection has improved the equipment's reliability. We have focused on user identification methods based on information technology. Scientific research on access control and management of this problem includes modeling visitor flow behavior for mass events and developing access control systems for monitoring visitor flow.

The questions of identification process organizing continue to be developed. The use of technical means allows automating the visitor identification process, but it requires registering all users in a database with identification tags [1]. There is a way to automate the user registration process through an online service; the visitor independently enters information for registration in the system, which does not allow verifying the accuracy of the provided information [2].

Materials and methods. The presence of problems in organizing access control determines the relevance of developing a technical solution capable of registering and identifying visitors without disrupting business processes [1]. The purpose of this research is to increase the efficiency of visitor's identification processes in educational institutions using information technology.

To solve these problems were used functional modeling and programming methods.

We suggest using mobile devices for identification and authentication in the access system. They are based on the use of chip cards, where a set of stored identification data can be automated in control mode [1] in educational institutions and can be used for technology transfer depending on the required level of security of the facility.

The project development involved combining identification devices, controllers, software, and blocking devices into one system [6, 7]. Cards and a device for their recognition – a proximity identifier reader – are also included. Together, they constitute an access control system [3, 8].

Identification devices comprise identifiers and readers. The identifier should determine the user distinguish them from other individuals. For example, a key fob with a specific chip distinguishes you from other objects; you have access rights where others do not. Another example is a PIN code; this is already identification, enter it, and you gain access [3-4].

Readers are necessary for reading and transmitting code information from the identifier to the controller. Most such readers have the capability of sound and feedback, allowing them to inform the user whether access has been granted or not [5, 8, 9].

Blocking devices are turnstiles that organize the passage of each incoming person one by one into the building (Figure 1).

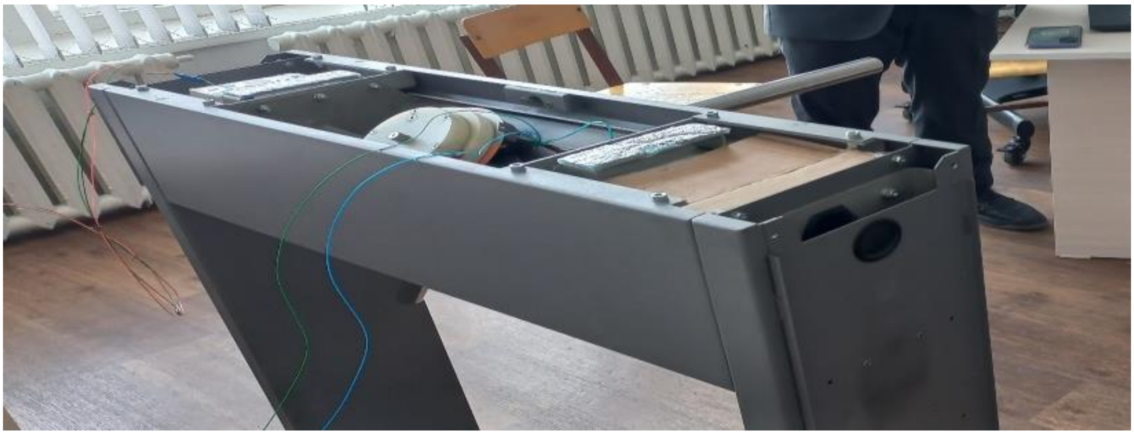

Figure 1. Turnstile, automatic rotation of the blocking slats is carried out due to the built-in electric drive

Controllers are microprocessor devices that perform event log storage, user database storage, and management of blocked devices [10, 11]. We used network controllers connected to a laptop with software [11, 12].

The purpose of the access control and management system is the operation of a software and hardware complex that automatically determines access rights to a facility. Automatic access control is implemented through a unique identification code (ID) of the subject. For example, the code of a certain information carrier - a chip card. Codes are stored in a database. If the code is not present in the database, it means access is denied. Each code corresponds to a set of access rights, such as permitted areas or time intervals. Based on the information about the user's code, the access control system makes decisions to allow or deny access, following the program's algorithm. If the program provides a positive decision, the control device is unlocked. After the user passes through, the device is locked again [7].

A chip card is a contactless card that has an electronic chip consisting of a receiver, an inductor (antenna), and an integrated circuit (chip), and it has a unique identification code stored in its memory. A contactless reader emits a radio signal at a frequency of 125 kHz-13.56 MHz and operates at a distance of 6-51 cm. When entering the range of this radio signal, the contactless card is activated, and a current appears in the coil, charging the capacitor, which supplies energy to the microchip of the integrated circuit.

The card (chip) sends a signal to the reader, which contains its unique identification code, based on which the proximity identifier makes a decision about granting or denying access [1]. The operation of the turnstile, automatic rotation of the blocking bars, is carried out through the built-in electric drive [1, 7, 13].

The identification procedure includes identifying the person entering the building based on the assigned identification attributes [7, 14]. The presented identifier is compared with the full list of assigned identifiers. The identification process model can be represented as follows:

suppose you have n access objects registered in the identification system. At the time of student registration in the identification system, their image is created, a set of reference values. This could be a series or pass number [15]. The task of identification is to determine whether the image p corresponds to exactly one element from the set of attributes. Access control and management tools (readers, code entry devices, controllers, electromechanical, electromagnetic, and mechanical code-based [8] turnstiles, control panels, matching devices), software applications solve this task (Figure 2).

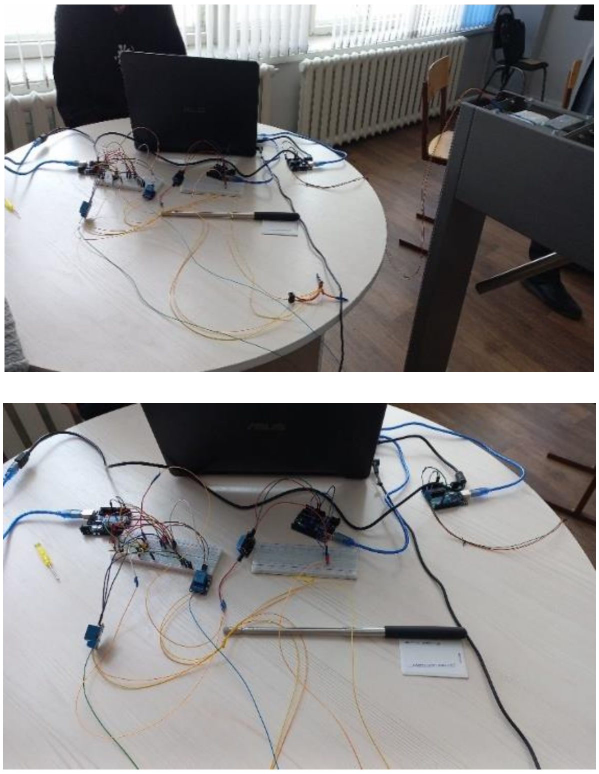

Figure 2. Implementation of the turnstile connection scheme

Results and discussion. The system provides access to a zone through a building entrance equipped with a controller, a device that can control and register visitors. The basis of the system, which makes a decision about access based on information received from the reader, stores data about users with access rights, which the controller uses to make decisions. If the access request is approved, the signal from the controller opens the barriers [16]. The reader receives information from the card for further transmission to the controller. There are many types of readers available today, both contact and contactless, and they work with different types of key cards.

We have explored a promising direction in access control and management systems - access via smartphones [16]. The software application for smartphone access combines the use of traditional access cards [17, 18]. Smartphones are intended for personal use and have their own security (password). There are several mobile applications available (installable from Play Market or Appstore) for this purpose, including ESMART Access, Parsec Card Emulator, PERCo Access, Proxway Mobile ID, and RusGuard Key.

To create a Python software application for organizing an access control and management system, you will need the following programs:

1) Flask or Django library for creating the application. Flask is a simple framework for creating web applications in Python, while Django is a more feature-rich framework for web application development. You can choose either of them depending on your hardware requirements.

2) A database to store information about users and their access. You can use SQLite, MySQL, PostgreSQL, or another database compatible with Python. Create tables to store user information, roles, and permissions.

3) An utility for standard authentication and authorization in Black or Django, or libraries like Flask-Login or Django-Allauth for additional functionality.

4) Create a design and layout using HTML and CSS, or use ready-made style libraries such as Bootstrap or Materialize.

Then use the available resources and functionality for each user role, implement the appropriate logic and functionality in your application. Do some testing to make sure it works correctly and meets your requirements. After completing the development of your application, deploy it on a web server to make it available for use [7-8].

Managing user sessions in a Python software application allows you to track user activity, save and update information about them during their session with the application. This helps maintain the user's state and provides access to various functions and resources within a single session. For this purpose, you can use libraries such as Flask-Session or Django Sessions.

Error handling in the application helps improve its fault tolerance and ensures smoother operation. Python offers various error handling methods, starting with the use of the standard try-except statement and ending with the use of error logging libraries such as Sentry or Loguru. Error handling allows you to control and manage potential issues in the application, prevent it from crashing, report errors to users or administrators for subsequent analysis and correction [8-9].

Logging in Python software is a practice for tracking events and processes within the application, as well as detecting and analyzing errors and issues. There are many logging libraries in Python, such as logging or loguru, which allow you to control log levels, write messages to different sources (files, databases, console), and customize log message formatting. Logging helps track user actions, monitor events, and identify and rectify errors in the application.

A Python program for access control through a turnstile can be developed using libraries and frameworks. Here is a template for a program that implements access control and management functions.

~~~~
```python
import time

def check_access(card_number):
# Проверка доступа для заданного номера карты
allowed_cards = ['123456', '789012'] # Заданные номера разрешенных карт
if card_number in allowed_cards:
return True
else:
return False

def log_entry(card_number):
# Журналирование входа пользователя
~~~~

~~~~
timestamp = time.strftime("%Y-%m-%d %H:%M:%S", time.localtime())
with open('log.txt', 'a') as log_file:
log_file.write(f"{timestamp} - Вход пользователя с картой {card_number}\n")

def open_turnstile():
# Открытие турникета
print("Турникет открыт")

def close_turnstile():
# Закрытие турникета
print("Турникет закрыт")

def process_card(card_number):
if check_access(card_number):
log_entry(card_number)
open_turnstile()
time.sleep(5) # Предполагаем, что пользователь будет проходить через турникет 5 секунд
close_turnstile()
else:
print("Доступ запрещен")

# Пример использования
card_number = input("Введите номер карты: ")
process_card(card_number)
```
~~~~

The template is further refined and improved for complex scenarios. Organizing a control and access system in a Python application allows defining different levels of access for users and controlling their access to specific functions and resources [10]. This can be achieved through authentication and authorization mechanisms such as JWT (JSON Web Tokens), OAuth, or a system of roles and privileges. The organization of a control and access system helps ensure the security of the application, prevents unauthorized access, and misuse of user rights.

Thus, handling user sessions, error processing, and logging in a Python application are important practices to ensure the security, fault tolerance, and reliability of the application, as well as user control and access. Using appropriate technologies and libraries simplifies and automates these processes in the development of Python applications (Figure 3).

A mobile device access control software application can be used to enhance security in various public places. The turnstile with a microchip is a key component in this scheme. The microchip reads and analyzes access card identification data. This information is used for authentication and access decision-making. The access control software configures access parameters, determines user rights, sets time restrictions, and identifies user locations. It also collects and displays statistics, including the number of authorized users and access denials, providing analysis of which users entered the premises and their locations. The software automates the access control process, eliminates errors, and ensures efficient use of resources and time.

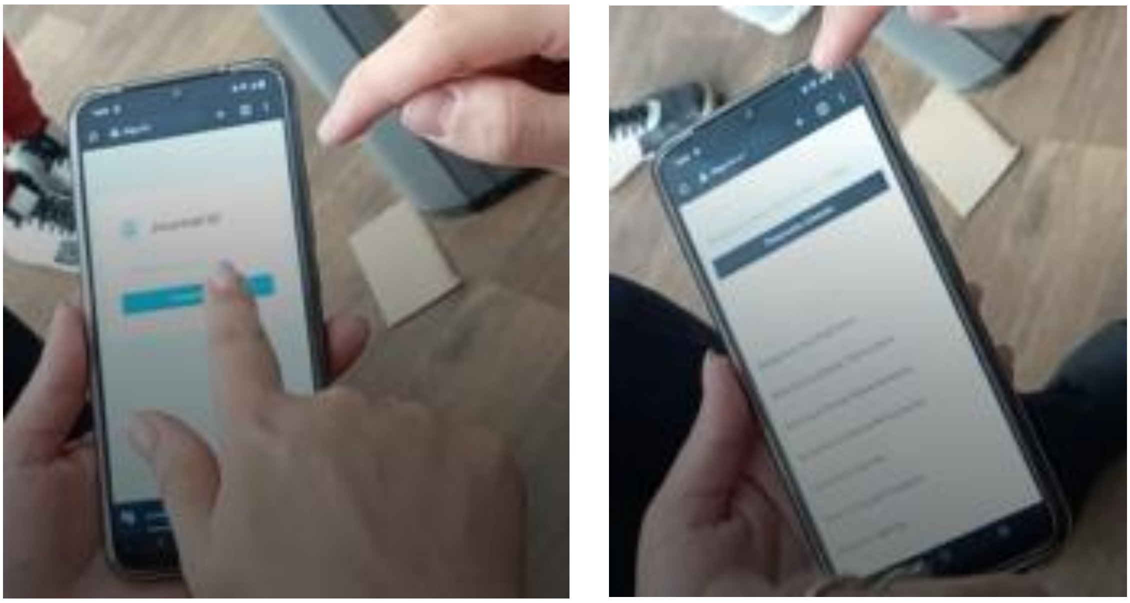

Figure 3. Access control software application on a mobile device

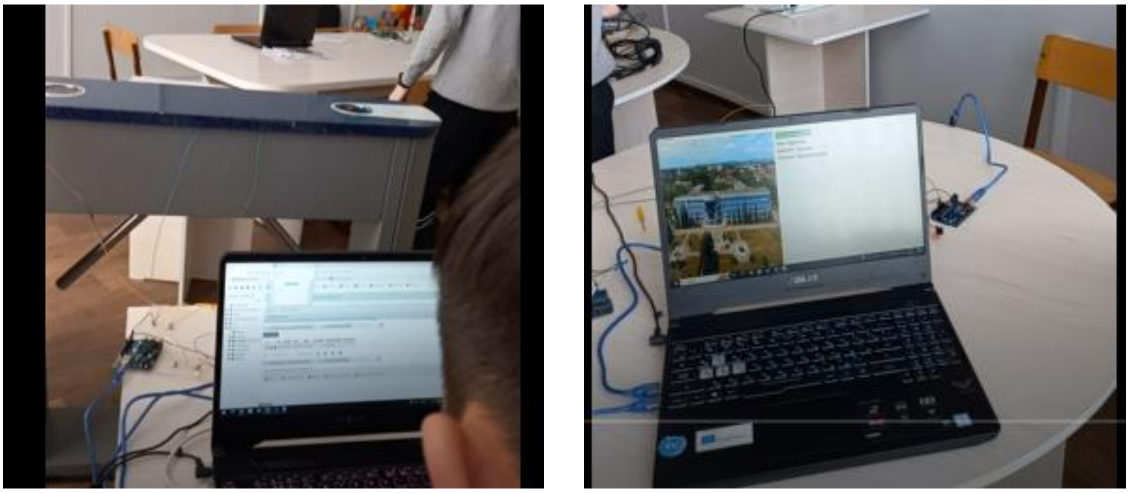

Figure 4. Software application interface for the controller

Conclusion. We have studied the technology of organizing access control using mobile devices, which can also be used to determine the location of students who have passed access control. The implementation includes both server and client components using Python and MySQL. The input and output data formats consist of a text SQL and a web interface. The software application interacts with other systems, facilitates data exchange and maintains unidirectional communication with data stored on the server. The Python software application and MySQL databases for student access control based on mobile devices work through a network connection in automatic mode. The application uses various resources and has an open module. It can be accessed from any device via the web interface. Supported data exchange protocols include HTTP, HTTPS, FTP, SFTP, SMB, XML, JSON, MPEG-2, MPEG-4, JPEG, GIF, PNG, H.264, H.265 and programming languages such as Python, SQL and HTML. The implemented type of computer is x86-compatible laptops, and the operating system is Windows.

The application provides access control and personnel management at the entrance and exit and informs them via a Telegram bot about their absence from the educational institution. Access to the room is carried out using a magnetic card.

Acknowledgements. This research is funded by the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Grant №. AP13268823 "Development of digital technology and intelligent system for non-contact measurement of body temperature using effective control points of images").

References

1. Iskakov A.Yu. Methodological and Program-Algorithmic Support for the Visitor Identification Process in Places of Mass Gathering. Dissertation... Candidate of Technical Sciences - Tomsk, 2016. – 140 p.
2. Medvedev A.M. Assembly and Installation of Electronic Devices / A.M. Medvedev. – Moscow: Technosphere, 2007. – 256 p.
3. Zaets N.I. Amateur Radio Constructions on PIC Microcontrollers / N.I. Zaets. – Kiev: "MK-Press", 2008. – 336 p.
4. Iskakov A.Yu. Identification Process Model in Access Control Systems // Bulletin of the Siberian State University of Telecommunications and Information Science. 2016;(1):93-98. (In Russian)
5. Alekseyev V.F. Principles of Design and Automation of Designing EAS: a textbook / V.F. Alekseyev. – Minsk: BSUIR, 2003. – 197 p.
6. Tikhonov A. A new protocol for Single Sign-on for the web / D. Gouriev, K. Belemuk // International Journal of Open Information Technologies. – 2014. – № 6. – P. 21-24.
7. Iskhakov A.Y. Identification process model in access control systems. The Herald of the Siberian State University of Telecommunications and Information Science. 2016;(1):93-98. (In Russian)
8. Tiki D.A., Novozhilova E. Resolving security issues and access control systems of the enterprise // Information Technologies and Systems: Management, Economics, Transport, Law – 2022. – № 2 (42). – P.125-129.
9. Schechter S. It's Not What You Know, but Who You Know: A Social Approach to Last-resort Authentication / S. Schechter, S. Egelman, R.W. Reeder // Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '09). – New York, 2009. – P. 1983-1992. – Doi: 10.1145/1518701.1519003.
10. Gouriev D. A new protocol for Single Sign-on for the web / D. Gouriev, K. Belemuk // International Journal of Open Information Technologies. – 2014. – № 6. – P. 21-24.
11. Belousov R.G. Choice of authentication algorithm based on the use of QR codes // Student Science for the Development of an Information Society: Collection of Materials of the VII All-Russian Scientific and Technical Conference. – Stavropol: Publishing House of SFU, 2018. – P. 220-222.
12. Grusho A.A. Safe Architectures of Distributed Systems / A.A. Grusho, N.A. Grusho, E.E. Timonina, S.Ya. Shorgin // Systems and Means of Informatics. – 2014. – Vol. 24. – No. 3. – P. 18-31.
13. Yakob D.A. Development of a research methodology for the features of information access control systems: dissertation Candidate of Technical Sciences: 05.13.01 / D.A. Yakob. – Yekaterinburg, 2013. – 163 p.
14. Principles of operation of access control system (ACS) [Electronic resource] - URL: https://manggis.kz/blog/princip_raboty
15. Review of ACS solutions / ACS: reviews and market snapshots of security. [Electronic resource] - Access mode: http://www.techportal.ru/review/#obzoryresheniy-skud.
16. Employee Monitoring Software / Software. – Text: electronic // Vellisa: [Electronic resource] - URL: https://vellisa.ru/luchshieprogrammyi-monitoringa-rabotyi (Access date: 09.06.2022).
17. Lugovtsova N.Yu. Reliability calculations of technical systems and technogenic risk: textbook / N.Yu. Lugovtsova; Yurginsky Technological Institute. – Tomsk: Publishing House of Tomsk Polytechnic University, 2019. – 342 p.
18. Turnstiles / Access Control and Management Systems // Vashtvmir [Electronic resource] - URL: https://vashtvmir.ru/turniketyiskud/ (Access date: 11.06.2022).