Informational Biometric Technologies at Educational Holding Activities for Digital Economy Conditions

Yelena Yu. Lukyanova[1] and Daniil V. Gorobets[1]

[1] *V.I. Vernadsky Crimean Federal University, Prospekt Vernadskogo 4, Simferopol, Crimea, 295007,*

Abstract

An educational holding is the modern perspective form of a process interaction for different economic units that are included in it and provide various services in an area of education. That form of work actualizes solutions for problems of security procuring when accessing informational resources. Digitalization of the economy and a regime of restrictions in the pandemic Covid-19 contributed to the transfer of peculiar processes and operations of the educational holding to an online format when it is necessary to provide the clear and strict identification of persons who participates in the educational process. Previously existing means that were used for these operations are no longer sufficient. It is required the new approach to security of educational activity. The article discusses prospects for applying information biometric technologies at activities of the educational holding for the digital economy conditions. Features, advantages, and security of identification by face, palm, and fingerprints have been determined. It is suggested to use Biosmart-Studio to automate this process as well as its integration with various programs and applications taking into account the digitalization of an educational process.

Keywords 1

Information biometric technologies, educational holding, digital economy, identification security, automation, integration

1. Introduction

Nowadays educational holding is the optimal form for processes of education and correlative interaction between structures that are involved in its system. It operates with multiple business structures and peculiar individuals. At the same time following the requirements of the digital economy, the part of these activities has been transferred online. Ensuring safety at the educational holding is the basis for its economic and social stability. It is necessary to define information technologies that can solve this problem comprehensively. The thesis mentioned above helps to formulate the aim of this article as research prospects for an appliance of the information biometric technologies at activities of the educational holding beyond the digital economy conditions.

2. Materials and Methods

To achieve the aim of this article were applied the scientific methods as such as content analysis, statistic analysis, structural analysis, technical and economic analysis, economical modeling, expert estimations, theory of constraints, and process approach. Also, there were researched specific papers on the dedicated topic [1-28] and statistical data.

Proceedings of VI International Scientific and Practical Conference Distance Learning Technologies (DLT–2021), September 20-22, 2021, Yalta, Crimea

EMAIL: lukianovahy@ukr.net (A. 1); gdv.80@mail.ru (A. 2)
ORCID: 0000-0003-2060-033X (A. 1); 0000-0002-3637-4624 (A. 2)

3. Analysis on Prospects for the Appliance of Information Biometric Technologies at Activities of the Educational Holding Beyond the Digital Economy Conditions

There are different approaches to the security of an organization in the digital economy conditions. Peculiar papers of various authors [1-30] disclose a few of them. Figure 1 demonstrates existing systems of identification and authentication that can be applied at the educational holding for the complex security of informational processes and their components.

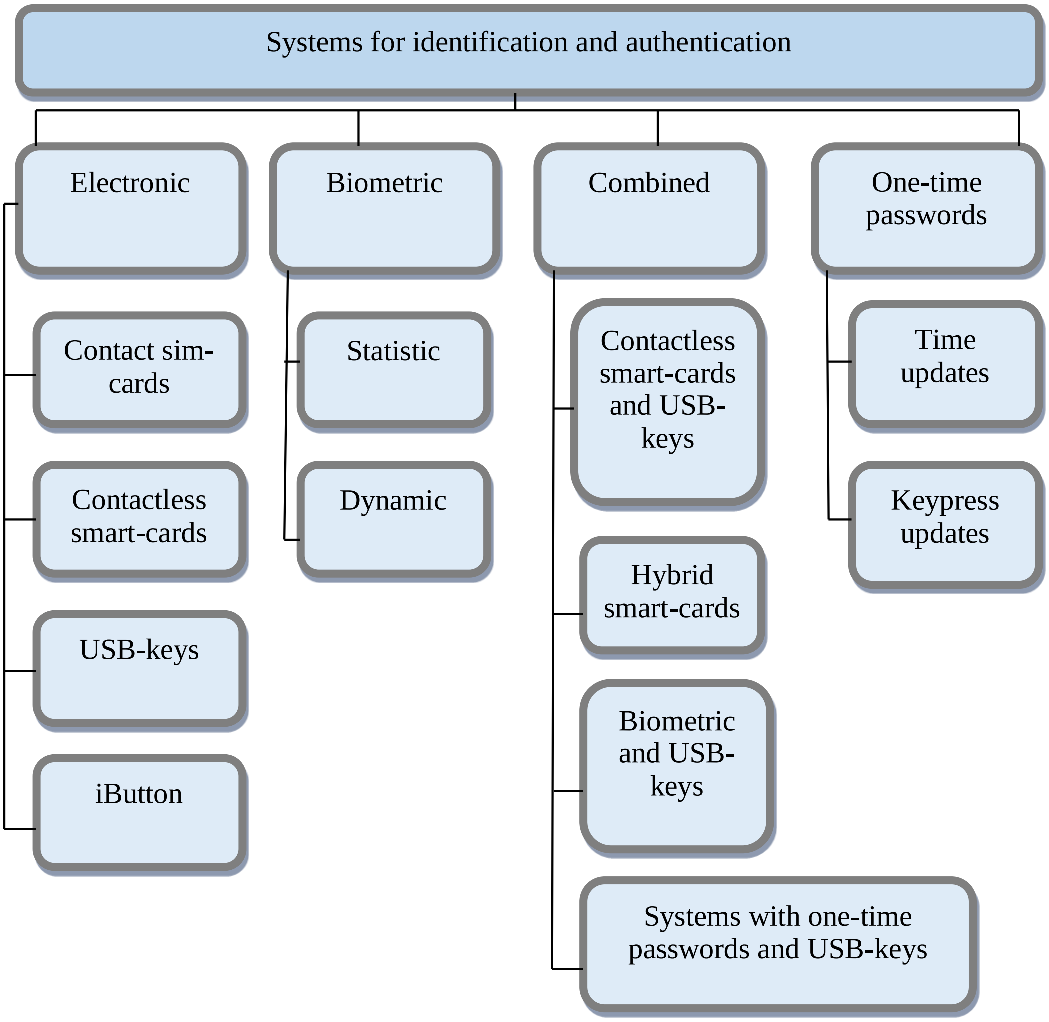


Figure 1: Systems for identification and authentication that can be applied for the educational holding

The best decision for the educational holding is to find an effective combination of mentioned systems. Nevertheless, the holding faces restrictions connected to the time of implementation for innovations on security also limitations on resources for it. This caused expertise on systems for the holding. It revealed that informational biometric technologies are the most appropriate ones for it. Its process is disclosed in Figure 2.

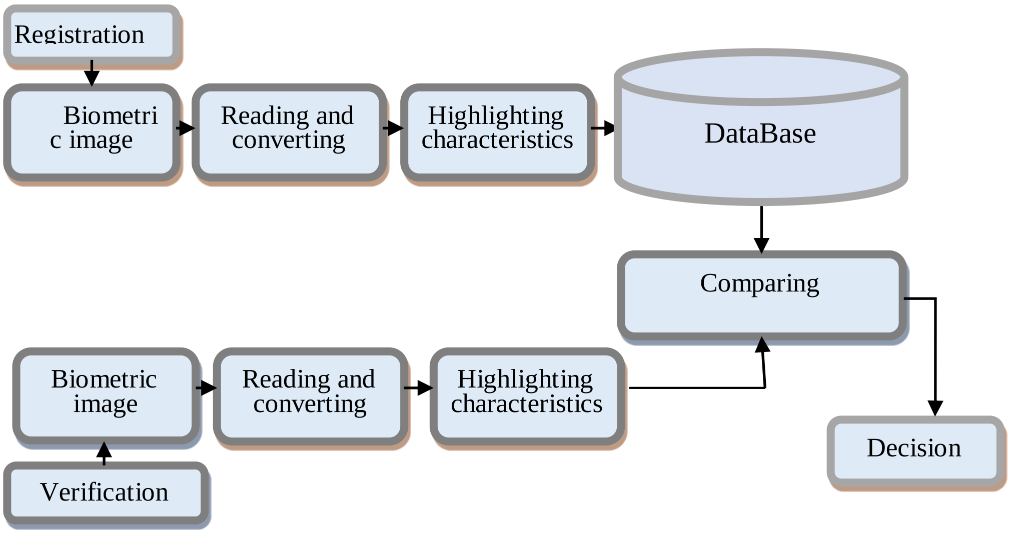
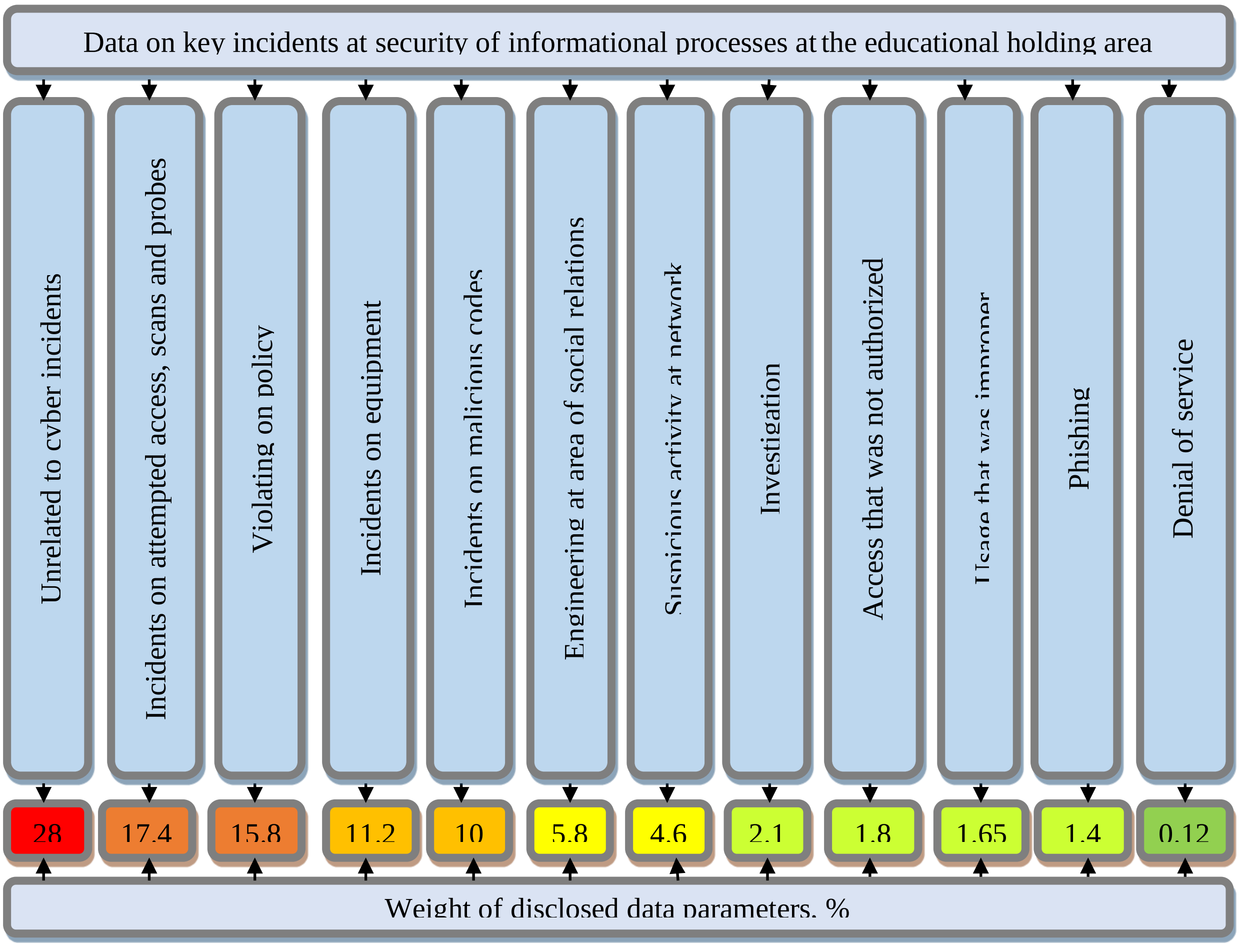


Figure 2: Process of the usage of informational biometric technology

The expertise also displays that there were multiple incidents at the security of informational process at the educational holding area. Key ones of them are illustrated in Figure 3.



Data on key incidents at security of informational processes at the educational holding area

Unrelated to cyber incidents	Incidents on attempted access, scans and probes	Violating on policy	Incidents on equipment	Incidents on malicious codes	Engineering at area of social relations	Suspicious activity at network	Investigation	Access that was not authorized	Usage that was improper	Phishing	Denial of service
28	17.4	15.8	11.2	10	5.8	4.6	2.1	1.8	1.65	1.4	0.12

Weight of disclosed data parameters, %

Figure 3: Key incidents at the security of informational processes at the educational holding

Figure 4 illustrates a diagram for the data that were disclosed in Figure 3.

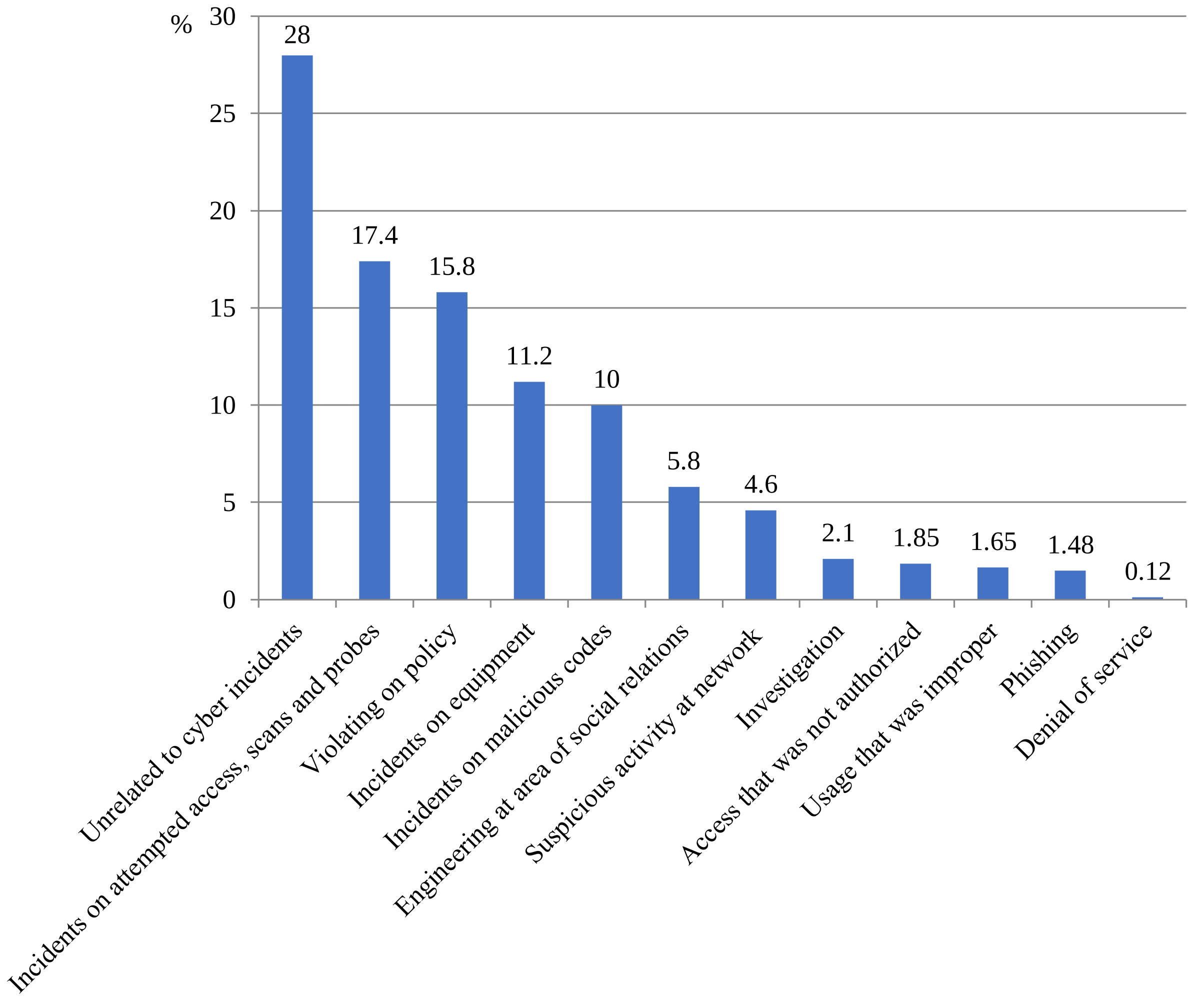


Figure 4: Diagram on key incidents at the security of informational processes at the educational holding

Security incidents at the structures of the educational holding are represented in Figure 5.

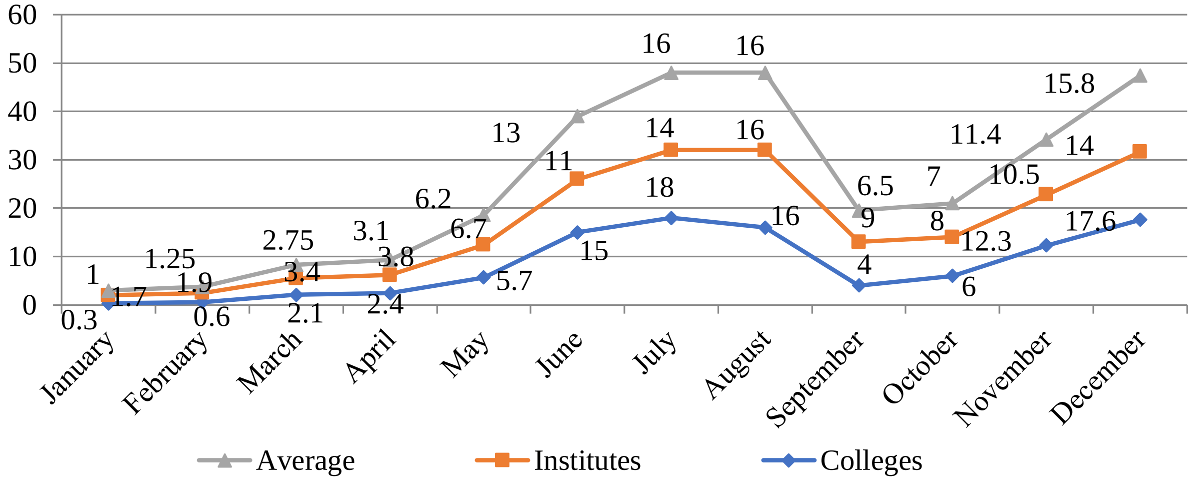


Figure 5: Security incidents at the structures of the educational holding by months (%)

Informational biometric technologies (IBT) are intended for identification by face, palm, and fingerprints. The biometric systems operate at the structures of control and administration of data and work time. They secure business resources from unsanctioned access and provide the maximal effective organization of personnel work. The IBT complexes are applied at all spheres of the economy and also are suitable for educational holdings.

Facial identification is based on the recognition of individual facial characteristics. A biometric terminal of facial identification is equipped with a stereo camera with an adaptive backlight. The 3D technology of shooting allows fixing characteristics of a face with a high level of accuracy at any luminosity even in the darkness. An image is coded as the mathematical pattern and then it is kept in a database. Further terminal identifies a person by comparing his facial characteristics with the patterns in the database. The advantages of this technology are grounded on the fact that the face of each person is inimitable and has more unique characteristics than a fingertip. The stereo camera identifies the person as absolutely reliable; it even fixes differences in the faces of siblings and people of any nationality. The facial biometry safely secures from a forgery in the contradistinction an RFID card that can be lost, forgotten, stolen, or handed over to a colleague. The terminal is equipped with a powerful processor therefore the identification takes less than half-second. Facial recognition is contactless, hygienic, convenient, and safe for health.

The palm identification is based on an identification of the person by an individual structure of the network of venous vessels underhand skin. The device scans the palm in multispectral infrared light and reads its reflection. Hemoglobin in veins absorbs part of the infrared radiation; therefore a pattern of blood vessels appears on a reflection. The mathematical algorithms convert the pattern to the digital code and pack it into an encrypted template file that is only 2 KB in size. To identify the person the device scans his palm and compares a resulting biometric template with the templates in the database. It is also a more secure way than the traditional RFID cards. This kind of recognition as well as the facial one is contactless, hygienic, convenient, and safe for the health. A condition of the hand does not matter because the vein scanner accurately recognizes the person by a dirty or damp palm or with cuts and calluses, and even a palm in thin medical gloves.

The identification by fingerprints is the scanning of an individual pattern of papillary lines on fingertips. The capacitive scanners register a difference in electrical potential between tubercles and depressions of a papillary pattern, the optical scanners recognize a fingerprint using the built-in camera. To identify a person the device matches one’s fingerprint with the patterns in the database. It has advantages at the recognition as such as the fingerprints are unique and don’t change throughout life, even if the skin is damaged, it is restored. Unlike the RFID cards fingers also cannot be lost, forgotten at home, stolen, or passed on to a colleague. The optical scanners are durable and resistant to damage. Scratches of the scanner don’t affect the image quality. The capacitive scanners are equipped with a heating system to confirm an identity even at sub-zero temperatures.

In the modern social and economic environment it is up-to-date to use complex information technologies for biometric identification at the educational holdings. Also, the very solution must have appropriate price and coverage. In the research, it was studied different program complexes for solving the problem. And such a solution can provide Biosmart Studio. It takes into account many years of experience at organizing access control and administration at many large and small economic units of various types of activity (from small offices and fitness centers to large factories and airports) at the Russian Federation, the CIS, and Europe. Biosmart Studio is constantly being improved to expand the capabilities and improve the convenience of working with Biosmart ACS [6].

Biosmart provides to the user's such kinds of activities as:

1. Centralized administration of operations for Biosmart controllers and terminals, setting their parameters and firmware updating.
2. Monitoring of performance of controllers and ACS terminals, registering and storing events (entry/exit of employees, actions of software users, updates, messages, malfunctions, etc.).
3. Creation, storage, deletion at ACS database of biometric data templates as well as other information about employees and departments.
4. Differentiation of access, creation of access scripts for different users (user groups, departments, enterprises).
5. Automated distribution of reports, messages, and reports by e-mail, SMS, or Telegram.

BIOSMART company produces face identification terminals with built-in protection against spoofing that is attempting to deceive the terminal using a fake image. A reliable anti-spoofing face recognition algorithm is the company's know-how. It ensures that the terminal does not react to a photo or a video. BIOSMART's joint projects with the operator of the Unified Biometric System have shown how face recognition operates in praxis. Thus the face recognition technology is successfully used at the bio-acquiring systems. The biometric image is used to approve a payment transaction or help to verify a customer's age for age-restricted purchases. As for the palm identification that was mentioned above it comes from that a vein pattern is not visible in normal light, so it cannot be photographed or faked. The BIOSMART's device scans the palm at several IR spectra at the same time, so it cannot be fooled with a silicone dummy. Only some significant parameters of the individual pattern of veins are encrypted in the digital template, so it is impossible to restore a full-fledged image of the hand from it. Even if an attacker gains access to the database, he will not be able to use it in any way. Wherever palm identification is used, this method has established itself as the most convenient and secure among all biometric identification methods. The devices for fingerprints identification also is provided by BIOSMART. Biometric information is stored in an encrypted form when identifier files contain only some significant parameters of a person's papillary pattern, thus it is impossible to recover a full-fledged image of a fingerprint from a file.

The biometric identification system of Biosmart consists of a wide range of equipment and allows the educational holding to organize an effective, reliable, and cost-effective access control and administrating system, personnel monitoring and control, and visitor identification. These systems can have any scale and complexity from local to network systems designed for large geographically distributed objects. The integration of video surveillance systems and Biosmart ACS opens up new opportunities in the field of biometric identification and the modern ACS solutions as increasing the security level of an object by adding information from the CCTV cameras to the ACS interface in the online mode; also reducing the resources of the security service to investigate incidents and prevent the fraud with working time due to simple access to the video archive from the ACS interface.

The add-on module "Integration with video surveillance" allows viewing live video from the cameras directly at the Biosmart-Studio software at the "Monitoring" module; it also adds the ability to view the video archive data from the Biosmart-Studio software in the "Logs" section of the ACS system events. The integration options are the binding of cameras of the video surveillance systems to the access points of Biosmart ACS, viewing the data of the video archive for any events of the access points from the Logs section of the Biosmart-Studio software, and viewing the live video in the Biosmart-Studio software from surveillance cameras. It can be used at security posts, checkpoints, and monitoring centers.

Today Biosmart ACS supports work with video surveillance systems such as Trassir, Macroscop, Linia, Intellect, and Axxon Next. In addition, the Biosmart-Studio v5 software provides the ability to connect the most IP cameras that support the RTSP exchange protocol. Integration options when working with the IP cameras include increasing the security level of the facility by adding information from the CCTV cameras to the ACS interface in online mode, binding the cameras to the points of passage or security area, viewing the video at the Biosmart-Studio software from the surveillance cameras. It can be used at any security post or checkpoint.

The use of the integration of 1C and Biosmart ACS allows linking salaries of employees to real data on their presence at workplaces, reducing labor intensity and influence of the human factor to the preparation of timesheets at 1C, automating data synchronization between 1C and the Biosmart-Studio software. The integration is based on the Biosmart-1C expansion module. The functionality of this module includes data transfer on an organizational structure and personnel of an economic unit from 1C to the Biosmart-Studio v5 software. The module automatically synchronizes the organizational structure of the business entity at 1C with Biosmart-Studio; it loads data on the input-output events from the Biosmart-Studio v5 software.

Also, it integrates data on sick leaves, vacations, and other reasons for absences of employees at workplaces for further registration at the report card and takes into account intraday business trips of employees, automatically calculates timesheets using a wide range of settings. The module fills out the standard configuration document 1C "Regulated timesheet" with the data that is evaluated based on correlating planned schedules and actual visits that allows calculating employee salaries based on the discipline of arrivals and departures. The Biosmart system can be integrated with any other system or a software package via API using the "API-integration" extension module. The integration interface uses the HTTPS / HTTP / TCP protocols and the XML exchange format, so developers can create the integrated solutions with the Biosmart-Studio v5 system regardless of technologies, programming languages, and applied operating systems. Using the Biosmart system API can be integrated with any third-party system (including different management systems of business structures, HR systems, CRM, and ERP systems); it automates data exchange between systems, transfers functionality from the Biosmart-Studio software environment to a familiar system, implements external client applications for the Biosmart-Studio software. Integration of Biosmart ACS with breathalyzers allows control sobriety of employees when they enter an economic unit or a work area. The Biosmart terminal identifies a person, and the breathalyzer determines the concentration of alcohol in the exhaled air.

An additional control factor can be integration with a video surveillance system or an installation of the "Biosmart + breathalyzer" device at visibility zones from the security points. The introduction of the Biosmart system integrated with the breathalyzer significantly reduces the number of injuries and emergencies at work. This process includes several actions. An employee confirms his identity on the biometric terminal, and then upon a signal on the terminal screen, he is tested on the breathalyzer. If the concentration of alcohol in the exhaled air exceeds the permissible value, the employee is not allowed to pass to the economic unit. The blocking event and the PPM level in the exhaled air are transmitted to the Biosmart-Studio v5 software. A notification about an attempt to enter an employee with an increased level of alcohol in the exhaled air is sent by SMS, e-mail, or Telegram. The alcohol content in the exhaled air is recorded at the system report on the alcohol testing of employees. The integration with breathalyzers is supported by the terminal for the veins of the palm Biosmart PV-WTC, Biosmart WTC2 fingerprint terminal.

The integration with Telegram adds an easy and simple way to interact with Biosmart ACS from a Smartphone or PC using the Telegram messenger. Managers will be able to receive events about passages of employees, system notifications, monitor the status of controllers, request their reports on working hours using the Smartphone with the Telegram application installed on it, and access to the Internet. The integration options provide to receive prompt notifications via Telegram about important events in the system (e.g., a failure in an operation of controllers), to monitor the status of the controllers – in the case of the abnormal events at the operation of the controller's notifications with the specific status of the controller are sent, to realize real-time tracking of passes of the employees through access points and sending the notifications about the employee passes, to allow them to request and receive reports on their hours worked.

Without exception, all Biosmart biometric identification equipment can be integrated into almost any third-party system using the SDK. Features of the SDK Device are the synchronization of lists of employees, blocking employees, administration of time modes, changing the parameters and operating modes of the controllers and the terminals, receiving an event log – passage of events and their system, receiving the event cache log – reading the events in real-time from the controllers and the terminals, the ability to change the state of the relay to control doors and turnstiles, registration of biometric templates from the controllers and the terminals, support for recording of biometric templates to the RFID card, etc. Key features of the SDK are cross-platform (support for Windows, Ubuntu, AstraLinux), easy integration of the Biosmart controllers and the terminals into the software of economic units, examples of use for common programming languages and support, and regular receipt of updates when new firmware for the controller are released.

Nowadays the Biosmart biometric identification equipment is integrated with the software of the following manufacturers that are listed in Table 1.

Table 1

Opportunities and integration of the Biosmart equipment with other program complexes

Program complex	Biosmart equipment	Opportunities and integrations
Intellekt ISB	Biosmart UniPass, Biosmart PV-WM, Biosmart PV-WTC, Biosmart DCR-PV	Control of access and evaluation of work time by applying biometric identification. Entering biometric templates, searching for the Biosmart devices, controlling and configuring devices, monitoring discrete inputs. Server authentication support. The Biosmart "UniPass" module uses such interface objects of Intellekt ISB as pass bureau, map, and log of events.

SIGUR	Biosmart 4, Biosmart 5M, Biosmart-WTC2, Biosmart PV-WTC, Biosmart DCR-PV, FS-80	The Biosmart equipment is connected to SIGUR controllers via standard Wiegand interface while each reader is connected to the IP network. The SIGUR server communicates directly with the Biosmart devices over the network. When working with the Biosmart readers this system supports few following access modes: only by biometric, only by card, by card, or by biometric, by several features.
Electronika Security Manager (ESM) hardware and software system	Biosmart 4, Biosmart UniPass, Biosmart PV-WM, Biosmart DCR-PV	Control of access and evaluation of work time by applying biometric identification. Registration and storage of biometric templates in the pass office of ESM. The "Template on map" mode has been implemented.
RUBEZH STRAZH ACS	Biosmart Quasar, Biosmart UniPass, Biosmart PV-WM, Biosmart PV-WTC, Biosmart-WTC2, Biosmart 4, Biosmart 5M	The Interaction of two systems is provided via communication channels of Ethernet and Wiegand. The uniqueness of the integration is that a separate server is still not required to operate with the biometrics in ACS: an information exchange is carried out between the RUBEZH STRAZH controllers and the “Biosmart” terminals/controllers. The following functionality is performed via Ethernet: obtaining the biometric signs from the controllers, entering information about users (full name, card number, etc.) and their biometric features to the “Biosmart” controllers, control on operating mode of the biometric controller, receiving events in the case of an unsuccessful identification. If the user is successfully identified, information about his number using the Wiegand protocol is transmitted to the RUBEZH STRAZH ACS that decides to grant access through the access point. All work with a cabinet filing and entry of identification signs is performed by the “Pass Office” operator at embedded Web software RUBEZH STRAZH.
RUBEZH FireSec R3	Biosmart 5M, FS-80	A Principle of operation of this integration is based on an actual connection of both the biometric reader and the MKD-2 module via Wiegand-26 interface and local network in which PC is located with installed FireSec R3 software. When a user is identified by the biometric reader, information is compared, received by MKD-2 via the Wiegand-26 interface from the reader as well as from the database at the FireSec 3 software. If data is relevant and consistent with each other, enter through this access point will be allowed.
NEYROSS platform	Biosmart 4, Biosmart 5M, FS-80	Integration of the Biosmart devices into ITRIUM software implies a provision of a software interface for the configuring and administrating access controllers, access points, peripheral devices, time zones, monitoring equipment status and obtaining information about current transactions, administrating databases of cards and fingerprints at the controller as well as the AWS service functions the “Bureau of passes” associated with automatic filling of fields the “Card number” and the “Biometric data”. The biometric templates are stored in passes and directly at the BOREY controllers. The

		size of the database for passes is limited by the memory of BOREY controllers – 100000. The "Map and biometrics” mode has been implemented.
REVERS 8000 ACS	Biosmart 4, Biosmart 5M, Biosmart PV-WTC, Biosmart DCR-PV, FS-80	The Biosmart devices are connected to the REVERS K2-8000R(E) / C2 32000R (E) controllers via the standard Wiegand interface. At the same time, “Biosmart” equipment is included in the object's IP network which is used to configure devices and centralized loading of the biometric feature templates from the REVERS 8000 software. Adding templates along with other data of employees (card, full name, position, department, etc.) takes place in the “Pass” program of the REVERS 8000 software via desktop USB-readers of Biosmart. When working with the Biosmart readers the REVERSE 8000 system supports the following access modes: only biometric, only card, card, and biometric for the unlimited number of users (server extension for Biosmart 4 devices).
Tsyrkonii-S2000 ISB	Biosmart UniPass, Biosmart PV-WM	Access control uses biometric identification. The registration of the biometric templates is made at the Tsyrkonii-S2000 pass office.

The suggested informational biometric technologies and the program complex provide a higher security level for the educational holding, reduce security risks and level of attacks.

4. Conclusions

In the economic digitalization context, the use of information biometric technologies provides the achievement of the necessary security level for the educational holding in modern business conditions. It is especially important to implement the combination of various biometric solutions for identifying people by fingerprints, palm veins, and faces. The options of Biosmart-Studio are intended for this especially considering its integration ability with other programs and applications. The Biosmart structures also effectively operate as part of the access control and time administration systems. They support protecting business resources from unauthorized access and organize the most efficient work of personnel.

5. Acknowledgments

This work is self-initiated and self-financed. Author thanks the committee of the conference for the participation possibility.

6. References

[1] S. Aanjanadevi, V. Palanisamy, S. Aanjankumar, An improved method for generating biometric-cryptographic system from face feature, Proceedings of the International Conference on Trends in Electronics and Informatics, ICOEI 2019, 8862741, pp. 1076-1079 (2019). DOI: 10.1109/ICOEI.2019.8862741.

[2] A. Abdellaoui, Y.I. Khamlichi, H. Chaoui, An efficient framework for enhancing user authentication in cloud storage using digital watermark, International Review on Computers and Software, 10(2), pp. 130-136 (2015). DOI: 10.15866/irecos.v10i2.5236.

[3] E. Abdellatef, E.M. Omran, R.F. Soliman, N.A. Ismail, S.E.S.E. Abd Elrahman, K.N. Ismail, M. Rihan, F.E. Abd El-Samie, A.A. Eisa, Fusion of deep-learned and hand-crafted features for

cancelable recognition systems, Soft Computing, 24 (20), pp. 15189-15208 (2020). DOI: 10.1007/s00500-020-04856-1.

[4] H. Abdi Nasib Far, M. Bayat, A. Kumar Das, M. Fotouhi, S.M. Pournaghi, M.A. Doostari, LAPTAS: lightweight anonymous privacy-preserving three-factor authentication scheme for WSN-based IIoT, Wireless Networks, 27 (2), pp. 1389-1412 (2021). DOI: 10.1007/s11276-020-02523-9.

[5] W. Abdul, O. Nafea, S. Ghouzali, Combining watermarking and hyper-chaotic map to enhance the security of stored biometric templates, Computer Journal, 63 (3), pp. 479-493 (2020). DOI: 10.1093/comjnl/bxz047.

[6] Biosmart-Studio, 2021. Url: https://bio-smart.ru/software-biosmart.

[7] D. Hidalgo, L. Cervantes, O. Castillo, P. Melin, R.M. Soto, Fuzzy parameter adaptation in genetic algorithms for the optimization of fuzzy integrators in modular neural networks for multimodal biometry, Computacion y Sistemas, 24 (3), pp. 1093-1105 (2020). DOI: 10.13053/CYS-24-3-3329.

[8] M.L. Lagunes, O. Castillo, J. Soria, F. Valdez, Optimization of a fuzzy controller for autonomous robot navigation using a new competitive multi-metaheuristic model, Soft Computing, 25 (17), pp. 11653-11672 (2021). DOI: 10.1007/s00500-021-06036-1.

[9] E.A. Abdel-Ghaffar, M.E. Allam, H.A.K. Mansour, M.A. Abo-Alsoud, A secure face recognition system, 2008 International Conference on Computer Engineering and Systems, ICCES 2008, 4772974, pp. 95-100 (2008). DOI: 10.1109/ICCES.2008.4772974.

[10] R.S.A. Abdalrahman, B. Bolat, N. Kahraman, A cascaded voice biometric system, Procedia Computer Science, 131, pp. 1223-1228 (2018). DOI: 10.1016/j.procs.2018.04.334.

[11] M. Abdallah, C. Fred, A. Farah, An authentication architecture dedicated to dependent people in smart environments, Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 4541 LNCS, pp. 90-98 (2007). DOI: 10.1007/978-3-540-73035-4_10.

[12] S.H. Abbdal, H. Jin, D. Zou, A.A. Yassin, Secure and efficient data integrity based on iris features in cloud computing Proceedings – 7th International Conference on Security Technology, SecTech 2014, 7023272, pp. 3-6 (2015). DOI: 10.1109/SecTech.2014.8.

[13] I.M. Abbadi, Digital rights management using a master control device, Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 4846 LNCS, pp. 126-141 (2007). DOI: 10.1007/978-3-540-76929-3_13.

[14] A.F. Abate, S. Barra, A. Casanova, G. Fenu, M. Marras, Iris quality assessment: A statistical approach for biometric security applications Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 11161 LNCS, pp. 270-278 (2018). DOI: 10.1007/978-3-030-01689-0_21.

[15] J. Andress. The Basics of Information Security: Understanding the Fundamentals of Infosec in Theory and Practice, Syngress, Burlington, 2011.

[16] R. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, Wiley, New York, 2020.

[17] R.E. Smith, Elementary Information Security, Jones & Bartlett Learning, Burlington, 2019.

[18] R.A. Grimes, Hacking Multifactor Authentication, Wiley, New York, 2020.

[19] R. Das, The Science of Biometrics: Security Technology for Identity Verification, Routledge, Abingdon-on-Thames, 2018.

[20] R.D. Labati, V. Piuri, F. Scotti, Touchless Fingerprint Biometrics (Series in Security, Privacy and Trust), CRC Press, Boca Raton, 2015.

[21] J. Wiles, T. Gudaitis, J. Jabbush, R. Rogers, S. Lowther, Low Tech Hacking: Street Smarts for Security Professionals, Syngress, Burlington, 2012.

[22] J.M. White, Security Risk Assessment: Managing Physical and Operational Security, Butterworth-Heinemann, Oxford, 2014.

[23] L. Bock, Identity Management with Biometrics: Explore the latest innovative solutions to provide secure identification and authentication, Packt Publishing, Birmingham, 2020.

[24] IFPO, S.J. Davies, B.D. Hertig, Security Supervision, and Management: Theory and Practice of Asset Protection, Butterworth-Heinemann, Oxford, 2015.

[25] M.I. Kaplan, B.P. Lang, S.C. Scheidt, Cybersecurity Defense and Operations, Phase2 Advantage, Savannah, 2021.

[26] W. Patterson, C.E. Winstin-Proctor, Behavioral Cybersecurity: Applications of Personality Psychology and Computer Science, CRC Press, Boca Raton, 2019.

[27] J. LeBlanc, T. Messerschmidt, Identity and Data Security for Web Development: Best Practices, O'Reilly Media, Sebastopol, 2016.

[28] S. Boonkrong, Authentication and Access Control: Practical Cryptography Methods and Tools, Apress, New York, 2020.