AUTOMATION AND COMPUTER-INTEGRATED TECHNOLOGIES

UDC 654.9:004.89-047.26:005.936.21(045)
DOI:10.18372/1990-5548.84.20195

[1]M. P. Vasylenko,
[2]A. R. Zahorna

SECURITY SYSTEM FOR OFFICE PREMISES WITH USE OF MODERN INFORMATION TECHNOLOGIES

[1,2]Aviation Computer-Integrated Complexes Department, Faculty of Air Navigation Electronics and Telecommunications, State University "Kyiv Aviation Institute", Kyiv, Ukraine
E-mails: [1]m.p.vasylenko@kai.edu.ua ORCID 0000-0003-4937-8082, [2]6294662@stud.kai.edu.ua

***Abstract*—*The paper analyzes the office premises and determines the required set of functions and structure of the security system, which includes a video surveillance subsystem, an access control subsystem, a burglar alarm subsystem, and a backup power supply subsystem. A detailed scheme of placement and interaction of components is proposed, and algorithms for the system operation are presented. The integration of the backup power supply subsystem with renewable energy sources ensures autonomous operation in the event of power grid failures.Office security is critical for protecting employees, property, and sensitive information by integrating physical and cybersecurity measures. Modern systems use advanced information technologies, such as remote, high-resolution video surveillance with autonomous analytics and biometric-based access control, to monitor, detect, and respond to threats efficiently. This technological integration enables real-time oversight and immediate action, significantly enhancing overall office protection.*

Keywords—Security; surveillance; motion detectors; access restriction; intrusion detection.

I. INTRODUCTION

Office security is now not only essential in today's environment, but also a crucial factor in determining an organization's stability and effectiveness [1], [2]. An office serves as a location for employees whose lives and health must be safeguarded from potential dangers, as well as a place to store property and critical information. Given this, it's the office's security system needs to be all-inclusive, capable of promptly warning of threats and responding to them [3] – [5], [7]. The most recent, intelligent security systems that not only offer physical safety but also boost the efficacy of protection against cyber threats are being developed on the foundation of modern information technologies, which are actively used in all facets of business [6].

Contemporary security technologies offer considerable enhancements to the protection of office environments by automating procedures and diminishing the potential for human-induced errors. Specifically, the deployment of high-resolution, remotely accessible video surveillance systems facilitates continuous facility observation, irrespective of on-site guard presence. Advanced video analytics possess the capacity to autonomously identify atypical events, including unauthorized entry or movement within restricted zones, enabling timely threat response [8] – [10].

An essential aspect involves the access control mechanism, employed to restrict entry to facilities solely to individuals with proper authorization. Contemporary approaches in this domain leverage biometric methods, notably fingerprint, retinal, or facial recognition, which markedly enhance security relative to conventional access cards or keys. Furthermore, access control systems can be interconnected with other elements of the security infrastructure, affording more versatile and efficient security oversight within the office environment [7].

Office security management systems leveraging advanced information technology can incorporate remote monitoring and control interfaces. This enables company executives or security personnel to observe real-time conditions, obtain security system status reports, and implement immediate actions, regardless of their location. Therefore, technological integration delivers both tangible and informational security, establishing a thorough system that optimizes office protection against all potential hazards [9], [10].

II. PROBLEM STATEMENT

A robust and enduring security infrastructure necessitates the development of an integrated framework encompassing a security alarm system, video surveillance, access management, and a redundant power supply. To optimize the effectiveness and caliber of this framework, contemporary information technology is employed.

III. SECURITY SYSTEM STRUCTURE

For the purpose of establishing a security apparatus, an office space encompassing 120 m², inclusive of five windows and a singular point of entry, has been designated.

The fundamental strategy for securing the office involves the fortification of entry points—windows and doors—through the utilization of magnetic contact sensors. Complementing this, infrared motion detectors and closed-circuit television cameras will monitor the interior, enhanced by electromagnetic locking mechanisms and entry facilitated via RFID reader technology.

The security infrastructure is composed of several operational modules: an intrusion detection system, a video monitoring system, an access regulation system, a supplementary power supply, and a central management server.

Consequently, the ensuing framework for a security system is recommended for the protection of the aforementioned office. (Fig.1).

- *The security alarm system includes*: IR – infrared motion sensors; MS – Magnetic contact sensors; CPU – Microprocessor; CDU – Receiving and conrol device; DRV – Servo drive modules; SRV – Servo drives; ALM – Siren.
- *The video surveillance system includes*: CAM – Video cameras; VDS – a separate computer for primary video processing and motion detection.
- *The access control system includes*: RFID – Reader; LCS – Lock control system; EML – Remote controlled electromagnetic locks.
- *The backup power system consists of*: BMS – Battery Management System; BAT – Battery.
- *MCS is the main control server*, which provides management of all system components, accumulation of video information, monitoring of system status and provides the possibility of remote access.

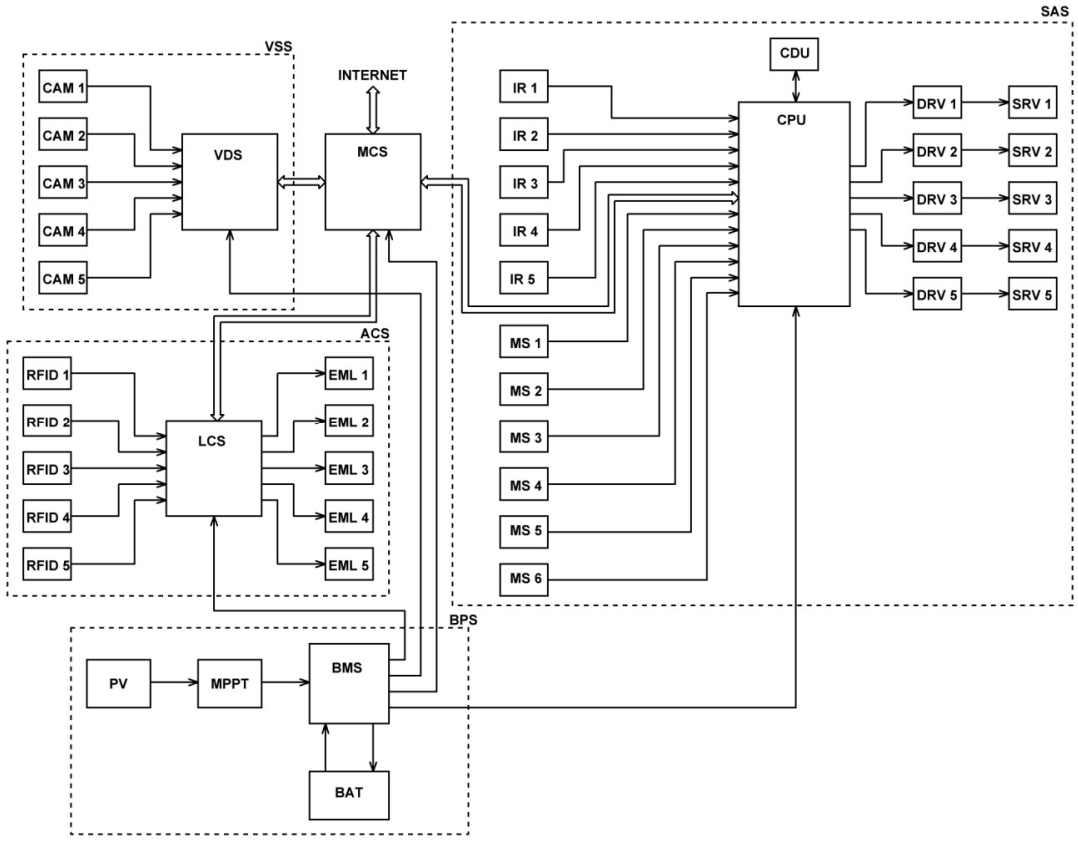

Fig. 1. The structure of the security system

Scheme of placement of the security system elements is shown in Fig. 2.

Infrared motion detectors are affixed in each room's corners at a 90° angle to the wall, positioned between 1.8 and 3 meters high.

Magnetic contact sensors are fitted onto window frames; an electromechanical reed switch is placed on the window's stationary component, while a magnet is attached to the movable part. The sensor placement mirrors that of doors.

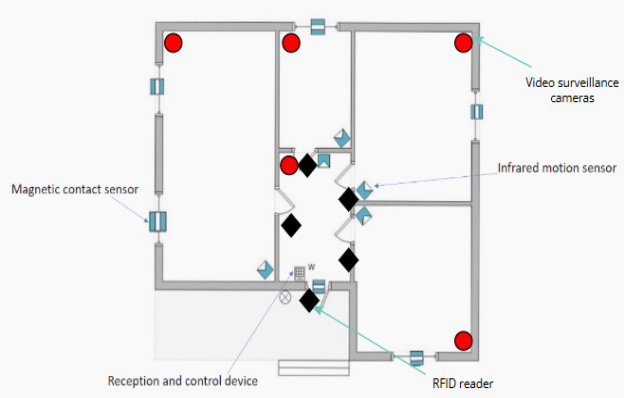

Fig. 2. Scheme of placement of the security system elements

Video surveillance cameras, angled 20–30° towards the ceiling, are aimed at the premises' entrances.

RFID readers are located at the entrances to the premises.

IV. System Control and Operation

The security apparatus is managed via a distant control interface, enabling users to activate or deactivate the system, acquire data pertaining to sensor conditions and operational modes, modify system configurations, and oversee battery status and charge levels. In instances where motion or magnetic sensors are triggered, the resultant signal undergoes processing by a microprocessor. This, in turn, generates a command signal for the notification mechanism and activates the corresponding indicator on the receiving and control apparatus. Furthermore, the security framework is regulated via a central control server, which additionally aggregates data concerning the system's condition.

The video surveillance infrastructure is governed by a video recording device, which undertakes preliminary image analysis and identifies movement within its scope. Subsequently, information pertaining to the detection of movement is transmitted to the primary control server, wherein video data from the surveillance cameras is also amassed.

The access management system, utilizing data obtained from RFID cards, verifies the eligibility of cardholders to enter designated areas. Upon confirmation of access privileges, a command is issued to disengage the electromagnetic lock securing the specified entry point. Information regarding access entitlements is communicated from the main server to the system's control computer. Moreover, directives to unlock specific locks can be initiated from the server.

The auxiliary power mechanism serves to ensure continuous functionality during episodes of mains power disruption. The system is initialized to its operational configuration utilizing the control unit's keyboard, which concurrently exhibits the prevailing system status.

Concurrently, the system initially assesses the state of the window opening sensors. In the event that all windows are sealed, the premises are armed. Conversely, should any window be ajar, the system generates a control signal directed towards the corresponding window servo, prompting it to effect closure. Upon successful window closure and the receipt of a confirmatory signal from the relevant opening sensor, the premises are armed. In instances where the window fails to close automatically, the control signal persists in its transmission to the servo; however, if after a duration of five seconds, no signal is forthcoming from the opening sensor, the control unit displays a corresponding indication, notifying the user of the necessity to manually close the affected window or eliminate any impediments obstructing its automatic closure.

During the system's operational phase, the activation of any motion sensors or the detection of window aperture precipitates the triggering of the detector and the remote transmission of a signal to both the security services and the primary monitoring server. A graphical depiction of the system's algorithmic framework is presented in Fig. 3.

The backup power system observes the existence of electrical flow within the external electrical grid; should this flow cease, the system transitions to battery power, a change communicated to the primary control server. Furthermore, the primary control server receives data pertaining to the present charge magnitude, the state of the battery (indicating whether it is charging or discharging), and the projected operational duration of the system's battery.

The continuous function of the video surveillance system results in the accumulation of video data for the preceding week on the primary control server, an action undertaken to optimize disk storage.

At the room's entry point, the access regulation system employs a reader that obtains identification data from the RFID pass, juxtaposing it against a repository of identifiers authorized for entry.

Command from the control computer opens the electromagnetic lock if the identifier is validated.

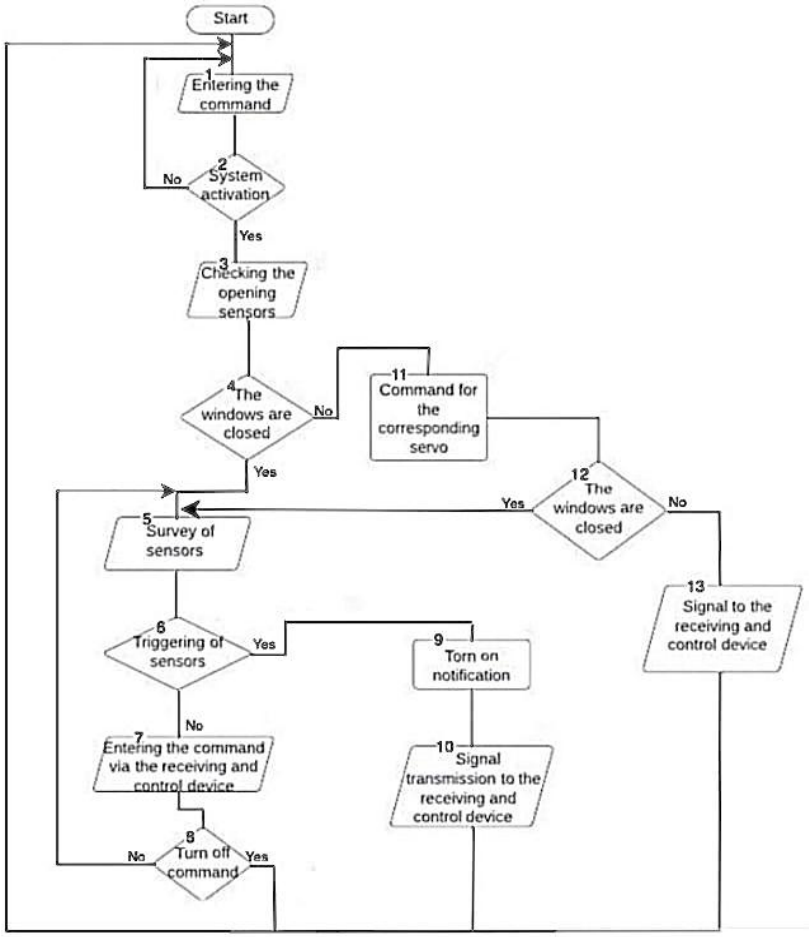

Fig. 3. Block diagram of the system operation algorithm

V. CONCLUSIONS

The integration of modern technologies into office security systems represents a significant step forward in ensuring the safety and efficiency of organizations. The proposed comprehensive system for a 120 m² office demonstrates a structured approach to addressing diverse security challenges by combining multiple components, such as security alarms, video surveillance, access control, and backup power.

The system's emphasis on automation and modern technologies reduces human error and enhances responsiveness to threats. Features like high-quality video surveillance system, access control and centralized management ensure both physical and information security. Additionally, the backup power system guarantees uninterrupted operation during power outages, further solidifying the reliability of the system.

REFERENCES

[1] J. Sullivan, & D. Andrews, *Modern Office Security Systems: Technology Integration for Workplace Safety*. – Springer, 2021, 356 p.

[2] R. Kemp, *Surveillance Technologies and Office Security: Trends and Challenges*. Oxford: Oxford University Press, 2020, 298 p.

[3] A. Chowdhury, & M. Rahman, "Access Control Systems: Principles and Applications," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 6, 2019, pp. 1563–1574.

[4] L. Smith, *Cybersecurity and Physical Security Convergence: Comprehensive Protection Strategies*, Elsevier, 2018, 402 p.

[5] *International Organization for Standardization (ISO). ISO/IEC 27001: Information Security Management Systems*, 2021.

[6] A. Bosco, & N. Kapoor, "Emerging Trends in Backup Power Systems for Security Applications," *Energy Systems Research Journal*, vol. 9, no. 3, pp. 210–220, 2020.

[7] National Institute of Standards and Technology (NIST). Guide to Physical Security Controls: Recommendations and Practices, 2022.

[8] P. Davis, "Automation in Security: The Future of

Office Safety," *Journal of Security Technologies*, vol. 15, no. 4, pp. 330–342, 2022.

[9] R. J. Fischer, & E. P. Halibozek, *Introduction to Security*. 10th Edition. Butterworth-Heinemann, 2019, 487 p. https://doi.org/10.1016/B978-0-12-805310-2.00019-6

[10] Honeywell Security Group. Comprehensive Solutions for Office Security: Technical Guide. – Honeywell White Paper, 2021.

Received January 08, 2025

Vasylenko Mykola. ORCID 0000-0003-4937-8082. Candidate of Science (Engineering). Associate professor.
Aviation Computer-Integrated Complexes Department, State University "Kyiv Aviation Institute", Kyiv, Ukraine.
Education: Kyiv National University of Technologies and Design, Kyiv, Ukraine, (2012).
Research interests: renewable energy sources, thermal noise based estimation of materials properties.
Publications: more than 40 papers.
E-mail: m.p.vasylenko@kai.edu.ua

Alina Zahorna. Student.
Aviation Computer-Integrated Complexes Department, State University "Kyiv Aviation Institute", Kyiv, Ukraine.
Education: State University "Kyiv Aviation Institute", Kyiv, Ukraine, (2024).
Research interests: technological processes automation.
Publications: 1
E-mail: 6294662@stud.kai.edu.ua.

М. П. Василенко. А. Р. Загорна Система безпеки офісного приміщення з застосуванням сучасних інформаційних технологій

У роботі проаналізовано офісне приміщення та визначено необхідний набір функцій і структуру системи безпеки, яка включає підсистему відеонагляд, підсистему контролю доступу, підсистему охоронної сигналізації і підсистему резервного живлення. Запропоновано детальну схему розміщення та взаємодії компонентів та наведено алгоритми роботи системи. Інтеграція підсистеми резервного живлення з відновлюваними джерелами енергії забезпечує автономну роботу в разі збоїв в електромережі. Система безпеки офісу має вирішальне значення для захисту співробітників, майна та конфіденційної інформації шляхом інтеграції заходів фізичної та кібербезпеки. Сучасні системи використовують передові інформаційні технології, такі як віддалене відеоспостереження високої роздільної здатності з автономною аналітикою та біометричний контроль доступу, для моніторингу, виявлення та ефективного реагування на загрози. Така технологічна інтеграція дозволяє здійснювати нагляд у режимі реального часу та негайно вживати заходів, що значно підвищує загальний рівень захисту офісу.

Ключові слова: безпека; спостереження; детектори руху; обмеження доступу; виявлення проникнення.

Василенко Микола Павлович. ORCID 0000-0003-4937-8082. Кандидат технічних наук. Доцент.
Кафедра авіаційних комп'ютерно-інтегрованих комплексів, Державний університет "Київський авіаційний інститут", Київ, Україна.
Освіта: Київський національний університет технологій та дизайну, Київ, Україна, (2012).
Напрям наукової діяльності: відновлювальні джерела енергії, оцінка властивостей речовин та матеріалів за власними електромагнітними випромінюваннями.
Кількість публікацій: більше 40 наукових робіт.
E-mail: m.p.vasylenko@kai.edu.ua

Загорна Аліна Романівна. Студентка.
Кафедра авіаційних комп'ютерно-інтегрованих комплексів, Державний університет "Київський авіаційний інститут", Київ, Україна.
Освіта: Державний університет "Київський авіаційний інститут", Київ, Україна, (2024).
Напрям наукової діяльності: автоматизація технологічних процесів.
Кількість публікацій: 1.
E-mail: 6294662@stud.nau.edu.ua