Security information systems constitute a significant application domain for the concept of situational awareness. The object of this study is security information systems for residential complexes. The task addressed involved devsigning an efficient, flexible, and adaptive structure to ensure situational awareness in security information systems. Unlike existing systems, this structure is based on the integration of intelligent agents, server services, and a central unit that interacts with the Internet of Things (IoT) network. The proposed system ensures the autonomy of intelligent agents, which perform specialized tasks using integrated intelligent sensors, while server services handle basic computational tasks such as machine learning, pattern matching, and model construction. The central unit aggregates information, implements reasoning procedures, and identifies situations for the entire system.

An architecture has been proposed that includes three main subsystems: video surveillance, access control, and operator service management. The essence of the results is the development of a flexible architecture that effectively combines IoT technologies with the situational awareness approach.

The research results were achieved by integrating innovative approaches such as the use of intelligent agents, machine learning, and situational analysis, enabling a flexible distribution of functions among system components depending on the specific task requirements. The distinctive features of this architecture facilitate the implementation of the situational awareness principle and support continuous system learning processes.

Given its modular architecture, the proposed system could be applied in extensive residential networks serviced by Internet providers, as well as in associations of co-owners of multi-apartment buildings. The formalization of architectural elements simplifies the process of designing and deploying systems, making them accessible for a wide range of applications in residential complexes by Internet service providers

Keywords: internet of things, system architecture, access control, video surveillance, security monitoring

UDC 004.8:007.52
DOI: 10.15587/1729-4061.2025.315248

DESIGNING THE STRUCTURE AND ARCHITECTURE OF SITUATION-AWARE SECURITY INFORMATION SYSTEMS FOR RESIDENTIAL COMPLEXES

Nataliia Kunanets
Corresponding author
Doctor of Sciences in Social Communications*
E-mail: nataliia.e.kunanets@lpnu.ua
Yuriy Zhovnir*
Yevhen Burov
Doctor of Technical Sciences*
Oleksii Duda
PhD
Department of Computer Sciences
Ternopil Ivan Puluj National Technical University
Ruska str., 56, Ternopil, Ukraine, 46001
Volodymyr Pasichnyk
Doctor of Technical Sciences*
*Department Information Systems and Networks
Lviv Polytechnic National University
S. Bandery str., 12, Lviv, Ukraine, 79013

Received 02.10.2024
Received in revised form 03.12.2024
Accepted date 16.12.2024
Published date 28.02.2025

How to Cite: *Kunanets, N., Zhovnir, Y., Burov, Y., Duda, O., Pasichnyk, V. (2025). Designing the structure and architecture of situation-aware security information systems for residential complexes. Eastern-European Journal of Enterprise Technologies, 1 (9 (133)), 6–23. https://doi.org/10.15587/1729-4061.2025.315248*

1. Introduction

Ensuring the safety of residential complexes is one of the key challenges of modern high-tech society. With the increase in urbanization and complications of housing infrastructure, the need to implement effective decisions for the protection of residents and their property increases. Conventional security systems do not fully meet the requirements of time, which creates the need for innovative approaches to the implementation of protection functions. Safety information systems, based on the Internet of Things (IOT) technologies, artificial intelligence methods and tools. They offer new opportunities to ensure reliable and comprehensive protection of residential complexes, apartment buildings in modern cities.

One of the key concepts that becomes rapidly relevant is the safety of residents of residential complexes. It is the information systems of situational awareness that can understand the context of the environment, identify threats, adapt to changes, and automatically respond to danger. The use of Internet of Things technologies in such systems greatly expands their capabilities, providing the collection and processing of large amounts of data in a real time.

2. Literature review and problem statement

The basic trend of development of modern information technologies is the introduction of methods and means of artificial intelligence (AI) in all domains of life and development of systems with situational awareness. Paper [1] provides an overview of publications that analyze methods and technologies that contribute to the development of situational awareness methodology. The areas in which this methodology is most commonly used from the collection of intelligence information to autonomous vehicles is defined, preferring to use situational awareness systems in the military industry. However, on the basis of the review, the researchers note the urgent need to design new tools for assessing situational awareness, on the basis of which further improvements could be made depending on the requirements of situational aware-

ness for a particular area of application. However, the paper only outlines the problem, emphasizes its complexity, and does not provide ways to solve it. Study [2] formally defines situational awareness as "the perception of elements in the environment within time and space, understanding of their value and projection of their status in the near future." Work [3] emphasizes that information systems, taking into account the situation, focusing on the ability to understand, interpret and respond to difficult situations from the real world. These systems are shown beyond basic data processing procedures and decision making, facilitating a deeper and more accurate understanding of the context. This enables them to act more reasonably in dynamic and unpredictable situations. Systems of this type are designed to better understand the situation that arise in the environment and the ability to respond to them in real time. This approach makes them convenient in use, including autonomous vehicles, smart cities, robotic complexes, and more. But the issues related to the peculiarities of architectural decisions of such systems remained out of the attention of researchers. The reason for this may be the complexity of the formation and architecture of such systems, which requires separate research.

A number of studies analyze the set of interrelated functions that must be implemented in the information system of the residential complex and note the complexity of such a system. Thus, the concept of architecture of the intellectual system in work [4] is defined as the structure of the system, its components and how they function together. It is noted that it combines hardware, software, databases, network, and other components. It is noted that one of the common ways of representing the architecture of the information system is a hierarchical structure, with three basic types of architecture of information systems: integrated, distributed, and mixed. However, the concept of "structure" and differences between the concepts "Structure" and "Architecture" is not outlined.

Paper [5] analyzes changes in the development of reasonable sensors, considers the evolution of these devices, and discuss the preconditions for the introduction of new highly effective sensors. Researchers have described the structure, characteristics, and functions of intelligent sensors with integrated intelligent capacity, in particular the features of the functioning of a typical intelligent sensor with distributed measurement nodes. This gave reason to choose the classes of new highly efficient sensors in the development of an information system of a residential complex as components of architectural solutions.

Some aspects of data processing in information systems based on IOT are analyzed in work [6]. The results of the study are very narrowly directed, do not take into account the features of specific environments and the need to interpret data for safety analysis. Paper [7] proposes a method of protection of information based on a zero trust strategy, which provides access only after verifying and identifying information and distributing information according to the target orientation. This approach is universal to some extent, but for information systems with situational awareness requires a significant expansion of information security methods.

Work [8] reports the results of research on intelligent agents that play a significant role in solving real security problems. It is noted that in multi-agent systems of action the agent directly influence those with whom it interacts. It is emphasized that conventional multi-agent security methods are based on reinforcement training. It is shown that they do not take into account the role of these localized interactions in coordination between agents. To solve this problem, the study presents an approach to safety based on optimization of structured coordinated proximal policy. The task of multi-agent patrolling is modeled as a distributed partially observed semi-Markovsky decision-making process with limited time. By accurately evaluating the contribution of the selected actions of each agent, this function helps improve coordination between agents. However, the problem of training and self-learning of intelligent agents and the formation of a knowledge base remained insufficiently studied. These aspects are important for designing information systems with situational awareness.

The concept of autonomous intelligent agents of cyber defense is outlined in [9]. Researchers analyze several scenarios that look at the types of threats that such agents may face and what actions will be potentially useful when forming a response. These agents are shown to be deployed in scenarios such as unmanned automated systems, power grids, communication networks in space and large-scale computing environments. This approach shows the expediency of using an intelligent agent capable of cooperating, sharing information, and adapting to a changing environment, which makes it a valuable tool for improving the level of safety and observation capabilities in systems with various settings. But there are unresolved issues related to the protection of housing since the proposed concepts are global and researchers do not present the possibility of their adaptation to the security environment of urban infrastructure.

The architecture of the information system "Smart House", proposed in work [10], has a typical sensory (perception) and applied level, but the proposed solution is at an intermediate level. The author highlights the problem of the great variety of users, changing situations and instability of the intelligent home environment and notes that this problem cannot be solved in conventional service-oriented systems. The authors propose to use systems based on the use of artificial intelligence methods and tools based on the rules for choosing the appropriate set of services. However, the study does not propose a combination of methods and means of artificial intelligence with a situation-awareness approach, which would undoubtedly increase the efficiency of the information system and its safety.

The integration of IoT information technologies with cloud services was analyzed in [11]. Centralized cloud architecture tends to consolidate computing resources and store data in several large centers of their processing. The increase in the number of IoT connected devices inevitably leads to excessive load on the network and delays in providing through services. The authors gave a mathematical model of distribution of services in cloud Internet networks as a problem of mixed flow with minimal cost, which could be effectively solved using linear programming methods. Such a globalized approach to the storage and processing of data is original but appropriate for cloud services and is difficult for use in local information systems. This very approach is used by the authors of work [12]. It is shown that approaches to identifying events in the "smart home" environment requires the use of a variety of sensors. It is noted that it is extremely important to use effective algorithms that could recognize new types of events, which facilitates the processes of data processing using uncontrolled training methods to identify base data models. The proposed processes of event recognition and forecasting make it possible to respond appropriately to user actions. However, researchers do not outline the possibility of scaling the information system and using it not only for individual homes.

Paper [13] presents the architecture of the information system "Smart House", which integrates contextual awareness. The proposed architecture of the information system has a five-level structure. The data collection level is respon-

sible for obtaining data from various devices and means of users, sensors, drives, and databases. The level of data management makes it easier to submit the required data to the level of context through the data collection component. All data collected on the first level are transmitted to the centralized server, where they are used for further analysis, visualization, and presentation. The level of context formulation synthesizes data from numerous sensors to achieve a complete understanding of the dominant situation. In addition, this level proposes the functions of aggregation, transformation, interpretation, filtration, and segmentation for improved data processing. The level of service generation generates relevant services that correspond to the context formulated at the previous level and/or any or reasoned context. The conclusion mechanism is based on access control protocols to ensure efficient safety. The level of service management is responsible for the supervision and administration of all components included in the system. This approach is quite original but cumbersome; at the same time, the problem of loss of information when moving from level to level is not covered.

Our review of the literature has identified a number of local problems related to the construction of residential safety systems. Key problems cover such aspects as the adaptability and scalability of systems [12], the effective use of Internet of Things technologies [11], cybersecurity [9], protection of privacy [7], as well as process automation in multicomponent intelligent systems [13]. Despite the significant successes in the development of individual technologies and modules, the task of building a holistic architecture of the information system that would integrate all these elements into a single comprehensive solution remains unresolved. The complexity of the integration of components, as intelligent agents, IoT-sensors, central data processing blocks and server services are often considered as separate elements that complicates integrated management, synchronization, and adaptation to living complexes. The scalability and adaptability are not inherent in most existing solutions that do not allow the system to scale according to the needs of large residential complexes, where the number of connected devices and the volume of data are constantly increasing. This creates significant challenges for the security system, which should be flexible and could adapt to changes in real time. Cybersecurity and protection of privacy are problematic with the increase in the number of connected devices, as the likelihood of cyber threats and leakage of confidential information increases. Most available systems are not sufficiently protected from modern threats, and the issues of protecting personal data of residents remain relevant. Process automation and situational awareness are important characteristics since security systems require high level of automation to reduce manual intervention and increase the speed of response to threats. However, existing solutions do not integrate the concept of situational awareness, which limits their ability to effectively respond to complex threats. Optimization of resources and productivity of intelligent security systems require improvement as they must perform complex computing procedures. In particular, machine learning and recognition requires considerable computing resources. However, not all systems could provide optimal load distribution, which could significantly affect the performance of their operation.

Based on the systematization of the above local problems, we shall state a general task – the need to design the integrated structure and architecture of the information system for the residential complex. The structure provides integration of intelligent agents, internal software service, central management unit, sensors, and knowledge bases into a single system. Architecture should be adaptive, scalable, and capable to respond effectively to real-time threats, maintain situational awareness, protect privacy and cybersecurity, as well as use computing resources optimally. Designing an integrated structure is critical for residential complexes. Modern security challenges require information systems for flexibility, stability, and efficient use of available technologies to ensure the safety of residents and protect their data.

All this suggests that it is advisable to conduct a study aimed at designing a security information system with situational awareness based on the technology of the Internet of Things.

3. The aim and objectives of the study

The purpose of our study is to design the integrated structure and architecture of information systems for residential complexes.

To achieve the goal, it is necessary to solve the following research tasks:

– to design a structure of a system that would include intelligent agents, internal software services, central control unit, sensors, knowledge bases, and IoT network;

– to investigate the features of the use of intelligent agents, internal software service, the central control unit in security systems;

– to design an architecture of a system that would include information system subsystems such as video surveillance, access control, and operator services;

– to analyze the functional features of subsystems in the information system of safety, which are set by separate groups of elements in subsystems and sets of relations given on them.

4. The study materials and methods

The object of our research is information systems for residential complexes security.

The research hypothesis assumes that the integrated structure and architecture of the information security system with situational awareness for residential complexes, based on the integration of IoT technologies, intelligent agents, and modern analytical methods, would increase the level of safety, ensure prompt response to threats, as well as flexibility of the system by optimally distributing functions among its components.

The need to build a security information system with situational awareness on the basis of IoT technology for a residential complex, not a separate apartment, is due to the scale of tasks and requirements for comprehensive safety of a large number of residents and infrastructure. Security systems for individual apartments have limited functionality and are not capable of providing effective coordination and centralized control at the level of an entire residential complex.

In the residential complex it is necessary to control access to joint areas (entrances, elevators, parking), ensure the integrity of the perimeter, respond to real-time anomalies, and manage infrastructure resources such as lighting, energy consumption, and emergency systems. The system must provide seamless integration between video surveillance subsystems, access control, alarm modules, and analytics.

The use of networks, laid by an Internet service provider, which systematically serves and meets the information needs of residents-members of the association of co-owners of apartment buildings (ACABs), avoids additional costs for the construction of a separate infrastructure for transmission and processing of data. This makes the implementation of the system appropriate, providing high capacity and reliability. With the use of information technologies of the Internet of Things, the system makes it possible to automate control, predict the emergence of potential threats based on data analysis, and ensure timely response to security incidents.

In addition, a security information system at the level of the whole complex allows ACAB executives to exercise centralized control, to provide access to analytics on resource consumption and safety status, as well as to ensure integration with residents oriented services. In turn, residents have benefits in the form of personalized services, such as remote access to surveillance cameras, ordering services in ACAB through mobile applications, or using web interfaces.

We design the residential complex security system using the infrastructure and software-technological platform by Astra company, which is the largest regional Internet service provider in the city of Lviv and provides for the formation of requirements, tasks, and technological specifications. Currently, there is a phase of experimental operation of the first stage of the specified system under actual conditions of several ACABs in the city of Lviv. The structure integrates intelligent agents, IoT devices, server services, and the central module of data processing into a single adaptive and scalable system. The architecture takes into account the functional features of each of the subsystems.

Restrictions could be described by several categories, including technical, integration, data safety, legislative. Technical restrictions relate to a network throughput that should be sufficient to transmit data from sensors and cameras in real time. The limited energy efficiency of IoT devices must be taken into account. Some autonomous devices have a limited battery time. The maximum number of simultaneously processed events may not exceed 150 events/minute. Integration restrictions imply compatibility between IoT devices, server components and cloud services, as well as compliance with safety protocols when transmitting data. Data safety involves encryption of data transmission channels, system access control (authenticating and authorization of users). Legislative restrictions determine compliance with personal data protection standards (GDPR, local regulations), compliance with video surveillance requirements in public and private places.

Assumptions relate to infrastructure, user behavior, and system parameters. The infrastructure promotes the system in a network environment with sufficient throughput, while all IoT devices are correctly configured and function in the set parameters. System users have basic skills in software interfaces, notifications are obtained and processed by persons with appropriate skills without delay. System parameters determine the regular updating of machine learning algorithms that provide accurate identification of situations, self-recovery of the system after short-term failures.

Assumptions relate to technological, operational, analytical aspects. Technological aspects suggest that all IoT devices support interaction standards (BLE, Wi-Fi, ZigBee, Z-Wave), cloud services provide sufficient computing power for real-time data processing. Operational aspects determine that the technical staff provides regular maintenance of the system, and in the case of peak loads, users could prioritize the process of processing critical events. Analytical aspects suggest that data analysis algorithms provide accuracy of threat identification in 95 % of cases, and typical scenarios of events meet the needs of residential complexes.

These data make it possible to formulate additional assumptions to improve the system. Subsystems must operate in real time with a uniform event flow. The data being processed must have the same difficulty for each event. Equipment (in particular, server components) should be used with average computing performance. These data and the assumptions formed will be used as a base to improve the system.

To investigate the structure and architecture of information systems for residential complex security, tools and methods are used to provide a comprehensive approach to the development of adaptive, scalable, and safe architecture. In the first stage of our study, we reviewed scientific publications on the results of research into the subject of information systems of security, technologies of the Internet of Things. situational awareness, as well as architectural solutions. To build the architecture of the information system, system analysis methods were used, which allowed us to evaluate the basic requirements for the system, determine the components, functions, and relationships between them. This made it possible to comprehensively study the complex information system, analyze their structure, functionality, relationships between components, as well as identify and formalize the requirements for the system. To build information system architecture, system analysis is fundamental because it provides a multidimensional approach to simulation. Structural modeling is used to design the overall structure of the system, which determines the interactions between intelligent agents, server services, the central module of data processing, and IoT network. Simulation is performed using notations in a unified modeling language (UML) and bock diagrams, which made it possible to visualize the structure and architecture of the system and its components. At the final stage, an empirical analysis of the work of the information system was performed, this provided the final adjustment of the architecture and the distribution of computing tasks among subsystems. The mathematical apparatus used in the study to describe concepts is based on the model of formalization of concepts interaction with the environment, data analysis, and decision making. It provides structured and unified representation of the components of the information system, their interconnections and functionality. The use of a set of orderly tuple elements is convenient for representing complex systems, in particular, those containing intelligent agents, as it makes it possible to take into account several interdependent aspects. The use of a tuple to represent concepts of the security information system makes it possible to organize all components in a single model, to represent both static and dynamic characteristics of the components of the structure and architecture of the system, formalize the interaction between components, build the basis for their software implementation. Thus, the use of a tuple to formalize concepts makes it possible to accurately describe all aspects of the system functioning and ensure its effective implementation.

The software used in the design of the residential complex information system is analyzed in detail in work [14]. Hardware includes intelligent devices and sensors, network equipment, server infrastructure, aggregation devices, client equipment. The category of intelligent devices and sensors includes CCTV cameras, traffic sensors, biometric devices. Dome, cylindrical, panoramic and pan, tilt and zoom surveillance cameras with resolution (Full HD, 4K), night vision support, IP66 for outdoor use are used. The information system contains different types of sensors. Movement sensors ensure the detection of activity in the observation zone and initiate video or alarm. Environmental sensors contribute to monitoring the state of the environment, in particular measure temperature, humidity, air quality. Access sensors integrate with door magnetic sensors or smart locks to control input/exit. Biometric devices, including fingerprints or face recognition scanners, monitor access to living quarters and general areas.

The network equipment includes the central router, switches, access network points. The central router performs the function of routing between the local networks of the residential complex and the Internet services provider. The router also provides balancing of load and quality of service to maintain the stability of the system. Switches are used to connect a large number of sensors, cameras, and intelligent devices through Ethernet. These are VLAN support switches, which make it possible to distinguish between areas of responsibility and ensure safety. Access networks are provided by IoT devices such as cameras and sensors, and support Wi-Fi 6 standards for high data transmission speed. The server infrastructure includes central server and cloud integration. The central server performs the functions of coordination of all components, processing, storage, and data analytics. The central server is characterized by high computational power, virtualization support to start multiple services and the use of RAID massifs to ensure data reliability. Cloud integration ensures the use of cloud services for backup, analytics, and scalability.

Among the aggregation devices, the leading role belongs to the central hub IoT as a physical device that performs the functions of data integration from heterogeneous sensors and devices. It provides the processing and routing of data from connected sensors and devices to other components of the system, such as servers or cloud services. The central hub is equipped with devices for connecting devices, such as Ethernet, USB, ZigBee, Z-Wave, built-in wireless modules, including Wi-Fi, Bluetooth, LoRaWAN, as well as a local data storage for temporary storage of information. Customer equipment includes various residents and security devices.

A hybrid infrastructure, which combines local servers, cloud services and developed network architecture, was used to deploy the security information system with situational awareness in the residential complex. Involvement of an ACAB internet service provider makes it possible to effectively use the existing infrastructure, minimizing the cost of implementing and maintaining the information system.

The use of these methods and research tools made it possible to design the integrated structure and architecture of the information system for a residential complex security, which is adaptive to changes, resistant to cyber threats, and capable of providing continuous monitoring of the safety state.

5. Results of investigating a security information system for a residential complex

5. 1. Structure of the residential complex security information system

Information systems in which situations are taken into account are a significant progress in the development of methods and means of artificial intelligence. Designing an information system that could identify and analyze situations is a rather difficult task. Such systems, in fact, should realize cognitive functions similar to those inherent in a person. This involves the use of contextual knowledge, learning processes, purposeful behavior, decision-making procedures, etc. The security information system must have the qualities of this nature, so it contains the functions of situational awareness under the conditions of uncertainty and unpredictability. It would function in a limited area, solve a limited number of tasks, and could implement an outlined set of situations for response, but would constantly learn by generating new situations.

Designing the structure of an intelligent security information system involves making decisions on the optimal distribution of intelligent sensors, computing capacity, location of decision-making centers. In doing so, the requirements for resources needed to perform various tasks, the need to respond under a real time mode are taken into account. A comparative analysis of information systems implemented on the principles of generative AI with intelligent systems has been carried out, which take into account real situations and scenarios (Table 1).

It should be noted that data collection could be performed from sensors, including video cameras, microphones, and sensors monitoring of environmental parameters. They could also pre-process data, filtering noise, improving the quality of the signal and detecting appropriate functions (such as movement, sound templates, etc.). Real-time data flows could be monitored to detect anomalies or suspicious actions, such as unauthorized access, unusual behavior, or the presence of objects where they should not be. In the event of a threat, agents could autonomously perform predetermined actions, such as closing the door, activating alarm, or redirecting camcorders to focus on a certain area of interest. For example, in response to a fire detected, an agent may unlock emergency exits and start a fire extinguishing system. Agents could analyze behaviors over time to determine potential safety threats. This may include tracking people in space or monitoring behavioral models that deviate from the norm. Agents could control and coordinate resources such as camcorders, unmanned aerial vehicles, or robotic patrols to optimize reach and provide effective monitoring of all areas. They could communicate and cooperate with each other to exchange information, coordinate actions, and make collective decisions. For example, if one agent identifies a potential threat, he or she may notify the nearest agents that they focus their sensors in a particular zone and exchange data to confirm the nature and scale of the threat. They could serve as intermediaries between the system and the operators, submitting data in a clear format and offering the appropriate actions. Thus, the use of intelligent agents in video surveillance systems generates significant advantages, in particular, in improving the level of efficiency of the system, its scalability, adaptability and efficiency of real-time response.

Table 1

Comparison of the characteristics of systems implemented on the principles of generative AI with AI systems that take into account real situations and scenarios

No. of entry	Generative AI	Situational AI
1	Focuses primarily on generating content (text, images, etc.) based on patterns generated from large datasets. While these models can produce impressive results, they often lack a deep understanding of context or the ability to intelligently interact with the real world	Goes beyond generating content by understanding real-world context and making decisions or taking actions based on that understanding. This means the transition from the generation of passive perception to active interaction with the environment
2	Operate mainly in the digital sphere, processing and generating messages based on textual data	Designed for interaction with the physical world, integration of sensor data and decision-making in real time. This includes not only understanding text, but also interpreting visual, audio, and environmental data to plan and implement appropriate actions
3	Although endowed with the ability to produce creative results, it lacks autonomy in decision-making procedures or in adapting his behavior to changing circumstances	Includes systems that can autonomously adapt their behavior, make real-time decisions, and interact with their environment in meaningful ways, demonstrating a significantly higher level of intelligence
4	Despite their complexity, large language models mainly deal with language and pattern recognition in structured or semi-structured data	In the systems of this class, a multidisciplinary approach is implemented, which integrates modern achievements in the fields of robotics, sensor technologies, peripheral computing and methods and means of artificial intelligence to create systems that are able to act autonomously in real situations and scenarios

One of the first steps towards the productive implementation of this kind of systems is the design of the structure of the information system, which determines how intelligent functions, the corresponding functional components are distributed, and their interaction is realized. The original paper aims to provide the structure of the security information system in a large modern city residential complex, providing the organization of processes of selection, storage, and processing of data, basic provisions and principles of work.

The peculiarity of the implementation of this kind of systems is that it is focused on the development and support of the Internet service provider operating in large home networks and maintenance of ACAB. The residential complex (RC) means the formation that is isolated from the living environment as a self-sufficient structural unit, which includes interconnected residential and non-residential objects and objects of engineering infrastructure.

The structure of the information security system is formed on the basis of relevant tasks. These include real-time monitoring of the state of the territory, video recording of events in the environment of a smart residential complex and storage of video materials, detection and analysis of suspicious activity, notification of residents about detected threats, maintenance of two-way communication between users and visitors, control of access to facilities and premises of the residential complex.

In order to complete the tasks set, it is necessary to comprehensively cover the territory with video surveillance, registration, and storage of video, detection of traffic and analytics. At the same time, it is necessary to provide remote access to the premises of the residential complex and the ability to manage them, resistance to external factors and protection against vandalism, round-the-clock control over access and urgent response to problematic situations.

Our analysis of the basic principles of construction of the intelligent information system for residential complex security revealed the following:

– it is implemented as a system with situational awareness, as it must ensure timely recognition of safety threats and response to them;

– the decision is made using knowledge of past situations, and the system will predict to act proactively and reflect on the possible development of the current situation;

– there is a constant updating of knowledge and coordination on the basis of analysis of data obtained from a large number of different types of sensors;

– it supports both local analysis and decision-making and analysis of the overall situation, coordinating the actions of components;

– requirements for computing resources are taken into account for various tasks and combinations of foggy, local, peripheral, and cloud computing will be used.

Before analyzing the structure of the proposed information system for residential complex security, we formulated the definitions of this concept and the tasks that it should fulfill.

Usually, a structure is understood as a pair consisting of a set of elements of a certain nature (components), as well as an order relation set on this set. We shall consider the structure of the information system to be an organized set of interrelated components that systematically interact, implement the processes of selection, registration, storage, transmission, processing, representation, and protection of information.

In the context of this study, the structure of an intelligent situation-aware security information system is understood to mean an organized set of components. They provide intelligent environmental monitoring procedures, data analysis and real -time safety control based on situational awareness. It includes intelligent agents, internal software services, central control unit, sensors, and knowledge bases.

The structure of a residential complex security information system (Fig. 1) contains the following components:

– intelligent autonomous agents – task-oriented autonomous devices integrated with intelligent sensors;

– internal software services, implemented as cloud services that perform resource-intensive calculations and are built in accordance with the requirements of service-oriented architecture;

– the central control unit that forms and analyzes the overall picture of the security situation, using information provided by sensors and services, as well as the knowledge provided in the knowledge bases.

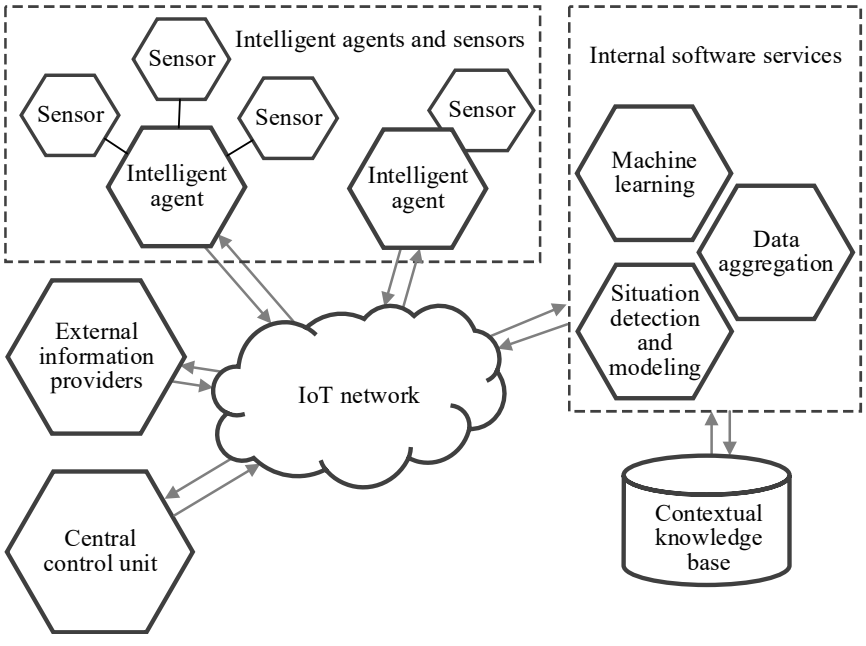

Fig. 1. Structure of a security information system with situational awareness

5. 2. Features of using structure components in security information systems

Intelligent autonomous agents. Intelligent autonomous agents are software or hardware entities capable of acting autonomously in the environment, making decisions based on the data obtained and performing tasks without human intervention (Fig. 2).

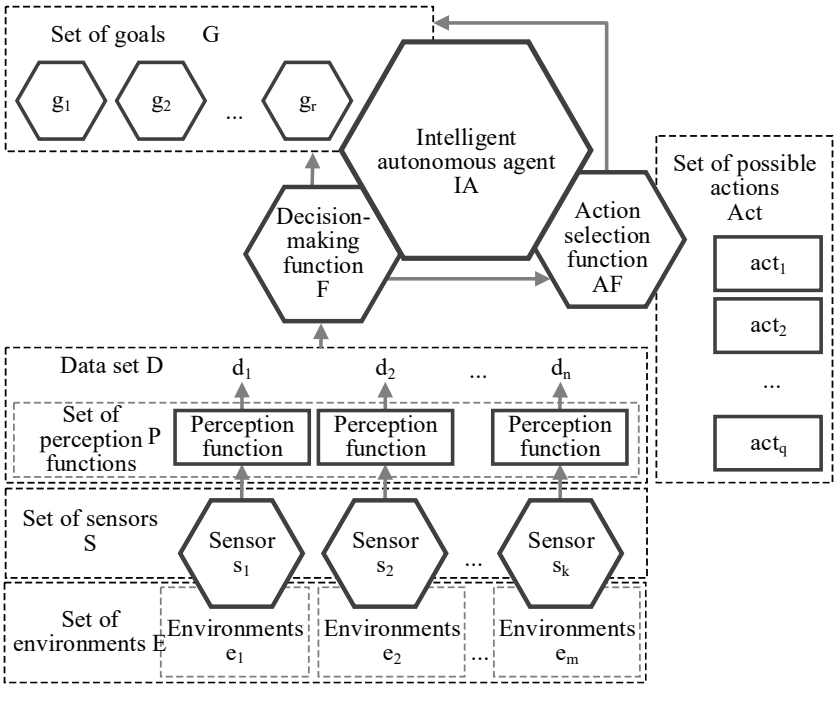

Fig. 2. Structure of the concept "Intelligent autonomous agent"

Such an agent is endowed with signs of artificial intelligence, which enables it to analyze situations, learn from experience, respond to changes in the environment, and cooperate with other agents or systems to achieve the goals. Intelligent agents analyze the situation in the environment based on data obtained from a sensor or group of sensors, interpreting them as parameters of objects in ontology. Sometimes it could implement functions related to automated actions under difficult or dynamic conditions. They usually interact with the environment and sensors and make decisions based on local data.

The concept of an "intelligent autonomous agent" is represented in the form of a tuple:

$$IA=\left(S,E,D,P,F,Act,G,AF\right), \qquad (1)$$

where S is the set of sensors used by the agent to obtain information from the medium $S=\{s_1, s_2, ..., s_k\}$, E is the environment, or the set of environments in which agents function $E=\{e_1,e_2,...,e_m\}$, D is a set of data collected by the agent from environments for analysis and decision-making $D=\{d_1, d_2, ..., d_n\}$, P is a function of perception that determines how the agent receives information from the environment. The set of perception functions $P=\{p_1,p_2,...,p_n\}$ corresponds to the set of data D, F is the decision-making function, Act is a set of possible actions that the agent could perform. $Act=\{act_1,act_2,...,act_q\}$, G is a set of goals that the agent strives to accomplish $G=\{g_1, g_2, ..., g_r\}$, AF is a function of choosing actions that determines what action the agent performs to achieve a goal based on data analysis.

The perception function P transforms the specific environment parameters (E) into data (D) that could be used by the agent for further analysis. Thus, each element of the medium $e\in E$ is converted to the corresponding data element $d\in D$. Formally, this is represented as $P:E\rightarrow D$, where function P establishes a clear correspondence between environmental states and the data obtained. F is a decision-making function that directly converts input (D) into specific actions (Act). Each element of

the set D is analyzed by the function F, and on the basis of the analysis selects the action from the set of possible actions Act. Formally, this is represented as $F{:}D{\rightarrow}Act$, where the function F establishes a correspondence between each element $d{\in}D$ and the action $act{\in}Act$. The AF action choice function takes as incoming data the data processed by the decision-making function F and determines the specific action from the set of possible actions Act that the agent has to perform. $AF{:}D{\rightarrow}Act$, where D is the data used for analysis and Act is a chosen action.

Sensors (S) collect data (D) about the medium (E). The perception function (P) converts information (Fig. 2) obtained from medium into data that the agent could use by treating them as parameters of ontology objects. The decision-making function (F) analyzes this data and determines the optimal actions (Act). The action selection function (AF) ensures that actions are taken to achieve goals (G).

The agent, using the function P, receives information from the environment E, which is transformed into data D. Based on the received data D, the agent uses the function F to determine the appropriate actions to be performed. The AF function enables the agent to choose and perform an appropriate action from a set of possible Act actions aimed at achieving a certain goal G. This representation describes the main elements of an autonomous intelligent agent, its functions and processes of interaction with the environment to achieve the set goals without human intervention. Intelligent agents are designed to perform such tasks as data collection, pre-processing, recognition, and interpretation of information about objects, detection of local anomalies, autonomous decision-making, mobility, and adaptability.

Agents are responsible for receiving data from their specific sensors (e. g., video cameras, microphones, thermal sensors). They can pre-process the data (e. g., filter, de-noise) to reduce the load on central systems. Agents also recognize and classify objects using information received from sensors and their common ontology. For example, agents distinguish people from pets or machines as different kinds of ontological individuals and populate the values of their properties using data from the corresponding sensors. Performing initial analysis to detect anomalies or events using peripheral computing reduces the need for constant communication with a central control unit. In critical situations (such as the detection of a fire or unauthorized entry), agents can implement immediate actions, such as sounding an alarm or locking a door. Autonomous decision-making presupposes the agent's ability to be goal-oriented, anticipate and prioritize actions. If the agents are mobile (e. g., drones, robots), they can adjust their position or focus based on detected events or changes in the environment. For example, an unmanned aerial vehicle equipped with a video camera and infrared sensors can patrol an object. It detects unusual heat signatures that may indicate a fire and sends an immediate alert, moving closer to the problem object for more detailed images.

Autonomous intelligent agents have considerable potential to perform local or peripheral computing, which makes it possible to reduce the load on central servers and increase the efficiency of the information system on a real time. Thus, they could use pre-trained models of artificial neural networks, created in the process of machine training in cloud services to identify anomalies and make decisions in specific contexts related to the specialization of this agent. They also send the data collected to the cloud services.

Another type of intelligent agents is specialized software agents using intelligent cloud services. Such services could identify objects, look for photographs of famous criminals in databases, or search the Internet information needed to make decisions. The main possibilities of such agents are to implement calculations on the periphery, increase the speed of processing and reduce delay, distribute data processing, confidentiality and data security, energy efficiency and resource optimization, self-study and adaptation. Autonomous agents are able to calculate directly on the devices or near the data collection, which reduces the dependence on cloud servers and network connection. This makes it possible to respond more promptly to local events, for example, in video surveillance systems or access control, where you want to immediately process the data obtained, such as cameras or identification, for immediate response to the situation. Due to the ability to calculate locally, agents reduce the delay in data processing, which is important for applications that require rapid response. This makes it possible to make real-time decisions, regardless of the speed of connection with central servers. Autonomous intelligent agents provide capacity for distribution of computing loads between several devices, which ensures the scalability of the system and reduces the risk of overloading the central node. This is especially useful in cases where many devices generate large amounts of data at the same time. Local computing makes it possible to maintain the confidentiality of the data because they are not transmitted to the cloud for processing. This reduces the risk of leakage or unauthorized access to sensitive information, which is important for health care or finance. Autonomous agents are capable of calculating, optimizing the use of energy resources. They could adapt the intensity of calculations depending on the available resources, which makes it possible to save energy and continue work even in limited capacity. Thanks to the built-in machine learning algorithms, autonomous agents could adapt to changes in the environment and improve their decision-making models based on the data collected. This is especially useful in situations where the conditions change rapidly and need to take into account local features (for example, changes in the network environment or user behavior). Autonomous agents analyze video and sensory data to identify threats, suspicious activity, and immediate threats.

Autonomous intelligent agents are an effective tool for local and peripheral computing due to the ability to make rapid decision-making, reduce delays, improve safety and scale. They open up new opportunities to create more reliable and independent systems, especially in cases where speed, confidentiality and autonomy of data processing are important. Thus, intelligent agents perform local tasks such as data collection, preliminary analysis, and prompt response. They act as components of the system that analyze events on a real time and transmit important data to higher levels.

Software services are important components of the intelligent security information system. Their use is due to the fact that some tasks in the system require considerable computational power, which could only be provided by the selected data centers. The internal software service as an element of the structure of the residential complex information system is a set of software components that work to ensure its safety. This service is responsible for managing subsystems, such as video surveillance, access control, and communication between different elements of the security system. It processes internal requests, controls resources, monitoring and automating security processes and interacts with the user interfaces to provide the necessary data to residents and administrators.

The structure of the concept of internal software service as an element of a more general structure of the information system for residential complex security (Fig. 3).

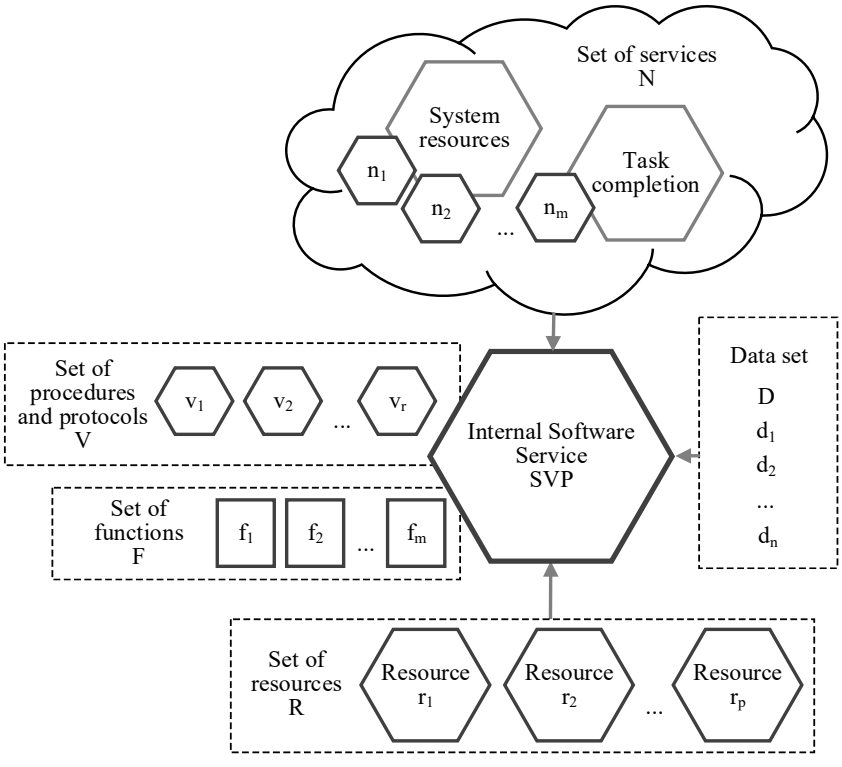

Fig. 3. Structure of the concept "Internal Software Service"

The formal recording of the concept of "internal software service" as an element of the structure of the information system for residential complex security is given by the tuple:

$$SVP=(N,F,R,M,V), \quad (2)$$

where N is a set of services implemented as cloud computing and providing resources for the system, ensuring the fulfillment of tasks related to security $N=\{n_1,n_2,...,n_m\}$, F – a set of functions performed by the service, determine how the service implements data processing and perform complex calculations to ensure the required security functions. $F=\{f_1,f_2,...,f_m\}$, R – a set of resources used by the functions (computing, memory, etc.), include the infrastructure required for service. $R=\{r_1,r_2,...,r_p\}$, M is a set of data processed and stored by the security and decision-making service. $M=\{m_1,m_2,...,m_q\}$, V is a set of procedures and protocols, rules that ensure the proper functioning of the service within the information system. $V=\{v_1,v_2,...,v_r\}$.

In-house software services are modular, composable, mostly using cloud resources and computing. They provide specialized functions in the system. Services interact with both agents and a central control unit, often managing more complex data processing tasks. Software services perform such tasks as data aggregation and fusion; creation of machine learning models; ensuring communication and coordination; real-time data streaming and storage; situation detection and notification management. Combining data from multiple agents helps create a holistic picture of the monitored environment. Hosting and running models provides pattern recognition, behavior analysis. Communication management between different agents ensures that they work together efficiently (e. g., task distribution, load balancing). Data streaming and storage management ensures important data is preserved and accessible for further analysis. Analysis of notifications from agents provides the ability to determine whether they require further action. Internal software services collect data from various video cameras and motion sensors. They run a deep learning model to detect suspicious behavior and generate alerts about potential threats. These services act as specialized processing units, taking on tasks that require more processing power, use complex algorithms, or integrate between multiple agents. They ensure the correct understanding of data in context and provide alerts or take appropriate action.

The central control unit is the core of the system, which is responsible for general control, decision-making, and in-depth analysis (Fig. 4).

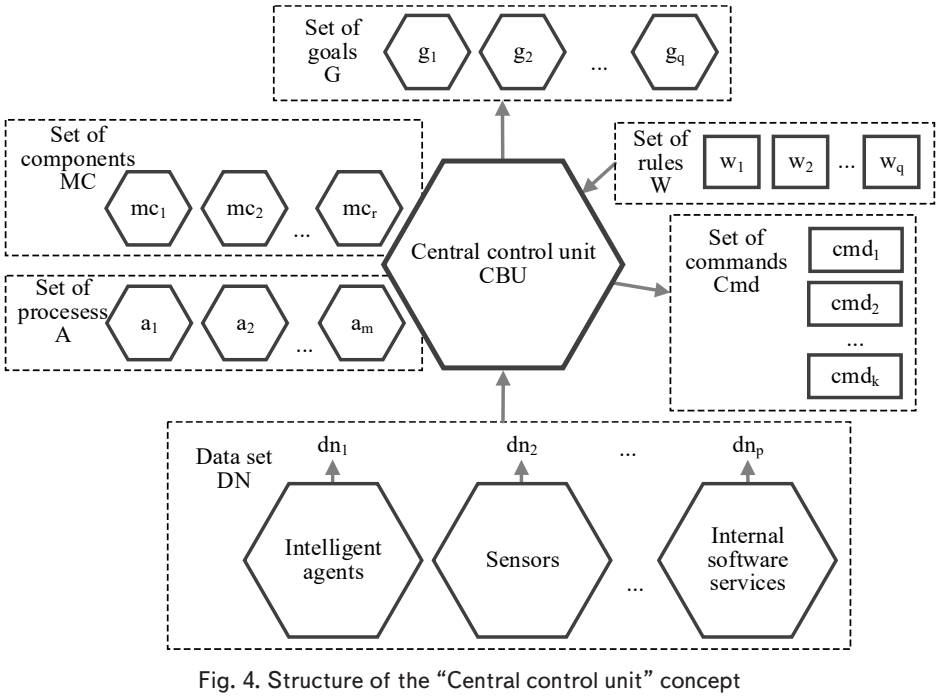

Fig. 4. Structure of the "Central control unit" concept

The concept of "Central control unit" is represented by the tuple:

$$CBU=(MC,DN,A,W,G,Cmd), \quad (3)$$

where *MC* is a set of components of the central unit that implement the main system control functions, provide hardware and software infrastructure for performing control procedures $MC=\{mc_1, mc_2, ..., mc_r\}$, *DN* is a set of data coming from sensors, intelligent agents and services of internal software, which are used for analysis with the purpose of forming general situational awareness $DN=\{dn_1, dn_2, ..., dn_p\}$, A is a set of processes performed for situation analysis, in particular data processing and anomaly detection, including in-depth analysis and threat detection. *A* associates each command with a specific component or subsystem that must perform an action $A=\{a_1, a_2, ..., a_m\}$, *W* is a set of rules that determine the logic of decision-making based on data analysis $W=\{w_1,w_2,...,w_q\}$, *G* is a set of goals or strategies that the system tries to achieve to ensure security, which determine the overall goal of the system, in particular, ensuring the safety of residents and responding to potential threats $G=\{g_1, g_2,..., g_q\}$, *Cmd* – a set of commands issued to perform actions that are determined as a result of analysis and decision-making $Cmd=\{cmd_1,cmd_2,...,cmd_k\}$.

The formal representation of the concept contains a characteristic of the processes of functioning of the central control unit, which performs the functions of collecting, data analysis, and decision-making to maintain the safety of the residential complex.

The interaction of the constituent elements of the concept involves the collection and analysis of data. The central control unit collects *DN* data from various subsystems. With the help of analysis procedures A, the central unit analyzes the collected data, identifies anomalies, threats, or other important events. Based on the analysis, using the *W* rules, the central unit decides on further actions. It forms commands *Cmd* and sends them to the appropriate components or subsystems. The presented formal model describes the structure of the central control unit, its interaction with other system components, and the decision-making process based on deep data analysis to support the overall security and efficiency of the system. In many cases, this concept includes human-machine interfaces for operators.

The functions of such a unit include global data analysis, decision-making support, policy management and strategy, centralized registration and reporting, resource allocation. The central control unit performs an in-depth analysis of the collected data, the integration of input from all agents and services to identify complex models or trends. The module provides support in the decision-making processes by operators, by synthesizing data and representing them in a convenient format, often with the help of information panels or intuitive-understandable visualizations. It implements and corrects policies, rules, and strategies of tracking on the basis of new requirements or ideas, conducts full journals and creation of audit reports and long-term analysis. The central control unit conducts a dynamic distribution of resources (corrects throughput, computing capacity) and coordinates tasks between agents and services to optimize productivity. The specified module receives a notification of unusual behavior revealed by the agent. It analyzes the event in context with other data (for example, recent security violations, current levels of threat) and decides whether to send to the scene of the security staff, or to send notifications to residents. The central control unit is the main module of decision-making at the highest level, supports the surveillance function and coordinates the overall strategy. It is it that makes the final decision in difficult situations that require a deep analysis of data or interaction with people. In the security information system, data flow from intelligent agents to internal software services, and then to the central control unit, where they are analyzed and processed. The central control unit sends corrective commands to agents and services, optimizing their work based on the analysis of new information. The degree of autonomy and centralization could be regulated depending on the specific situation and the required rate of response to threats.

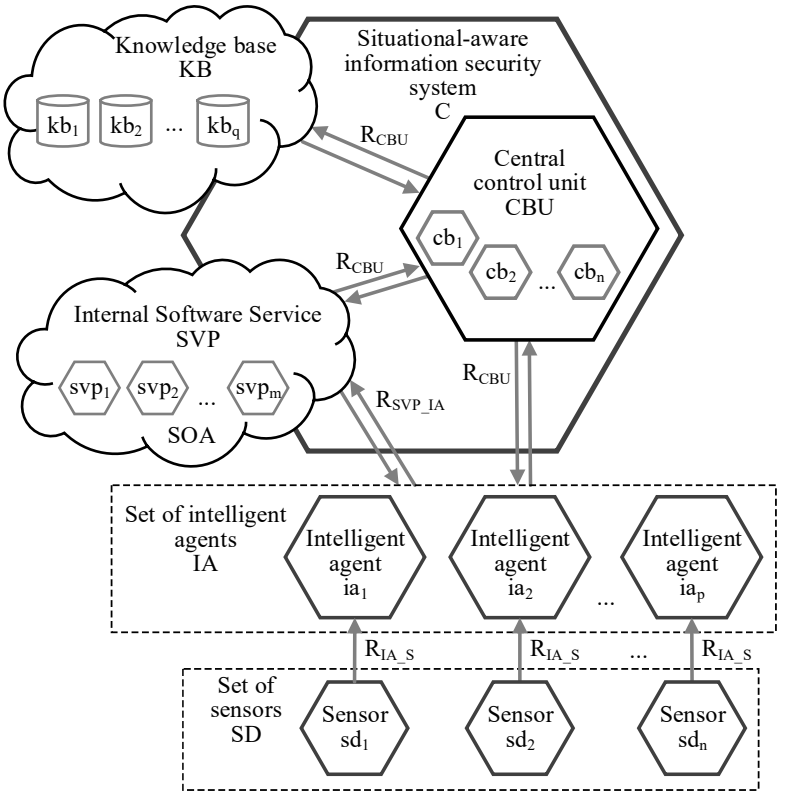

Fig. 5. Structure of a situation-aware security information system

The structure of an intelligent situation-aware security information system is shown in Fig. 5:

$$C = \langle IA, SVP, CBU, SD, KB \rangle, \quad (4)$$

where *C* is the structure of a situation-aware security information system, *IA* is intelligent agents, a set of autonomous devices focused on performing certain tasks and using data received from sensors $IA=\{ia_1,ia_2,...,ia_p\}$, *SVP* – internal software services provision implemented as cloud services that perform resource-intensive calculations in accordance with the requirements of the service-oriented architecture $SVP=\{svp_1,svp_2,...,svp_m\}$, *CBU* – central control unit responsible for forming an overall picture of the situation and analyzing information received from sensors, agents and services $CBU=\{cb_1,cb_2,...,cb_n\}$, *SD* – a set of sensors integrated with intelligent agents and providing data on the current situation $SD=\{sd_1,sd_2,...,sd_n\}$, *KB* – knowledge base used by the central control unit as expert knowledge to analyze the situation and make appropriate decisions $KB=\{kb_1,kb_2,...,kb_q\}$.

The relations available in the system among the components of a security information system are given as follows. Relationships between sensors and agents (R_{IA_SD}) consist of selecting data from sensors with intelligent agents:

$$R_{IA\_SD} \subseteq IA \times SD, \tag{5}$$

where *IA* is an intelligent agent, *SD* is a set of sensors.

The interaction between agents and the set of sensors (R_{IA_SD}) is defined as a set of pairs in which each agent (*IA*) transmits the sensor data (*SD*) to the service to perform the calculations. The interaction between services and agents (R_{SVP_IA}) is determined primarily by the implementation of the internal software service of the calculations based on the data formed by the relevant agents:

$$R_{SVP\_IA} \subseteq = SVP \times IA, \tag{6}$$

where *SVP* is an internal software service, *IA* is an intelligent agent.

Interaction between internal software services and intelligent agents (R_{SVP_IA}) is defined as a ratio in which the internal software service (*SVP*) receives data from the intelligent agent (*IA*) and performs the corresponding calculations.

The interaction between the central module and other components (R_{CBU}) implies that the central control unit interacts with intelligent agents, internal software services, and knowledge base for the implementation of the situation analysis processes:

$$R_{CBU} \subseteq = CBU \times (IA \cup SVP \cup KB), \tag{7}$$

where *CBU* is the central control unit that provides data analysis and decision-making, *IA* is intelligent agents that collect and transmit data, *SVP* – internal software services that perform calculations, *KB* – knowledge base that provides storage and access to the information required to analyze the situation. Intelligent agents (*IA*) collect data from sensors (*SD*) and transfer them to internal software services (*SVP*) for further processing. Internal software services (*SVP*), implemented as cloud services, perform resource-intensive calculations, and the results are transferred to the central control unit (*CBU*). The central control unit (*CBU*) uses information from agents, services, and knowledge of knowledge base (*KB*) to form a general picture of the security situation and decision making. This model describes the structure of the safety system components, their relationships that ensure effective security management.

5. 3. Architecture of security information systems with situational awareness

Unlike an individual "smart" building intended for living mainly individual families, large residential complexes, focused on the location of communities and numerous diverse groups of residents, face many specific problems. This requires the installation and maintenance of more complex and reliable infrastructures.

The architecture of a security information system means the conceptual model of an information system, which determines the components and their interaction, functions, as well as methods and means of integration with the external environment. The architecture specifies as the components of the system interact as they integrate with other systems and how the functions of ease of use, scalability, safety, and efficiency of the integral information system are implemented (Fig. 6).

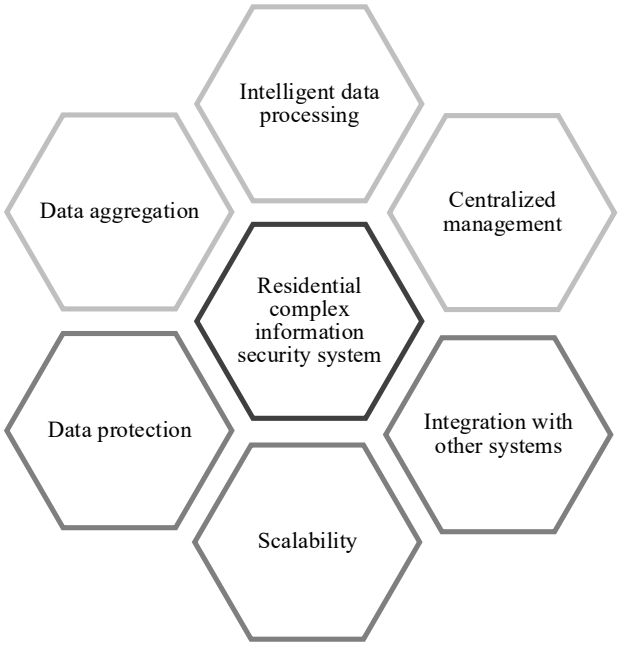

Fig. 6. Functional features of the information system for residential complex safety

The architecture of a residential complex security information system contains a number of components (Fig. 7). They provide compliance with such requirements as scalability, the availability of multiple access points, video surveillance coverage of common spaces, the processing of large volumes of data and managing them, exterior response to problematic situations. The architectural solutions for a security information system should be scaled to adapt to the growing number of residents, devices, new buildings in the respective residential complexes.

It is assumed that the system can process the growing data traffic, increase the number of simultaneous connections. Unlike a detached house with limited entry points, an apartment complex has multiple access points, including gates, lobbies, garages, and individual units, etc. Effective security solutions must include the management and control of these points. Common areas such as gyms, swimming pools, and parking lots require additional security measures. This includes surveillance and access control to prevent unauthorized entry and ensure the safety of residents in common areas. Managing data from numerous devices and sensors in a large community is significantly more difficult than in a single house intended for one family. Coordinating emergency response in a large community is more complex, requiring robust communication systems and protocols to ensure rapid and effective response to incidents. In addition, security systems in residential complexes must be integrated with the systems of local law enforcement and emergency services.

Formally, the architecture of a security information system of the residential complex is represented by a tuple of sets specifying individual groups of elements in the subsystems and sets of relations set on them:

$$IS = (VS, AC, MS, PR), \tag{8}$$

where *VS* (Video Surveillance) – video surveillance subsystem

$$VS = (C, M, S, A, V, R_{VS}), \tag{9}$$

where C is video cameras, M – microphones, S – sensors, A – analytical algorithms (detection of movement, face recognition), V – video streams, R_{VS} – rules of interaction with the central module.

CCTV subsystem (*VS*) collects data with cameras, processes them with analytical algorithms, and interacts with other subsystems through the central module.

AC (Access Control) – access control subsystem:

$$AC = (ID, B, L, P, R_{AC}), \tag{10}$$

where *ID* – identification data (cards, biometry), B – database, L – log files, P – access control rules, R_{AC} – response to events (locking).

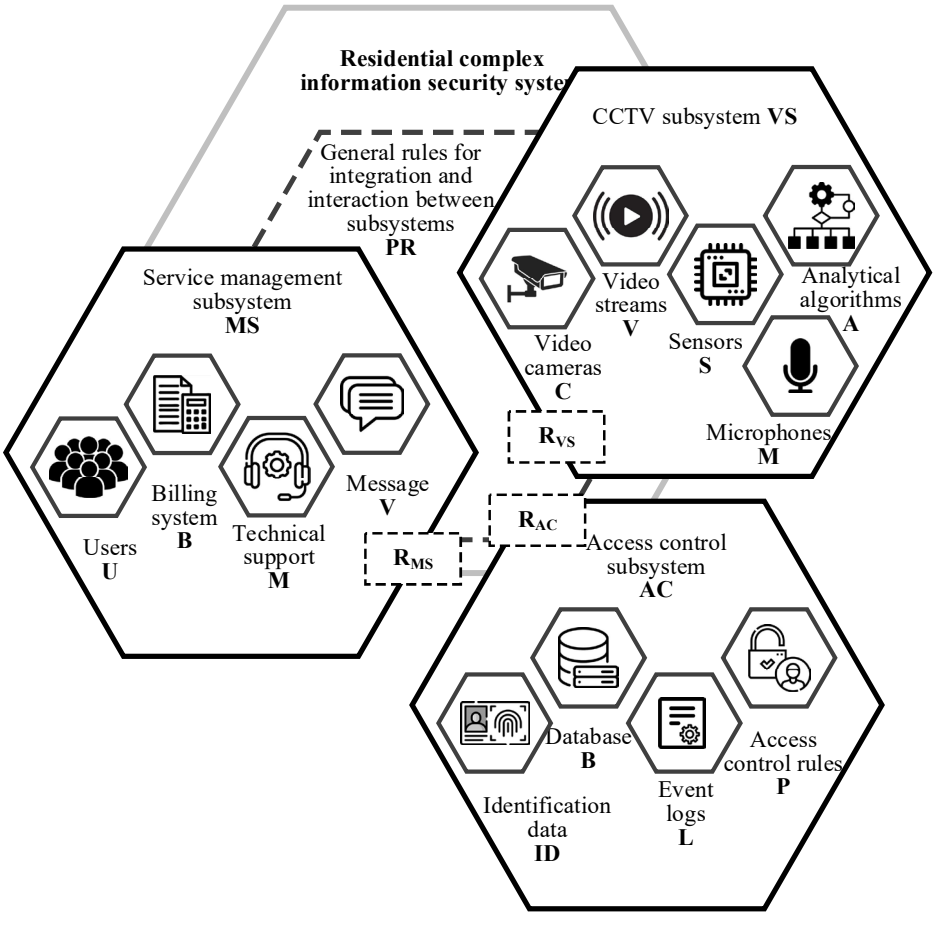

Fig. 7. Architecture of an intelligent situation-aware information system

The access control subsystem (*AC*) regulates access to premises, stores events, and could automatically block access in the case of threat.

MS (Management Services) – subsystem of service management:

$$MS = (U, B, T, N, R_{MS}), \tag{11}$$

where U – users, B – billing system, T – technical support, N – messages, R_{MS} –service management rules.

The operator's service management subsystem (*MS*) implements the processes of managing users, their subscriptions, service, and provides information services, in particular messages.

PR – general rules of integration and interaction between subsystems:

$$PR = \{PR_{VS}, PR_{AC}, PR_{MS}\}, \tag{12}$$

where RP_{VS}, RP_{AC}, RP_{MS} are the rules of integration and interaction of each of ythe subsystems.

These rules define how subsystems interact with each other and with the central control unit. Formalism comprehensively represents the main components of architecture and determines how they interact with the purpose of proper implementation and maintenance of security functions in the residential complex. This, in turn, makes it possible to clearly describe the components of the system, their functions, inter-component relationships, as well as record the main restrictions, which forms the reliable basis for the implementation of the processes of analysis, design, and practical implementation of the laid functionality.

5. 4. Functional features of subsystems in a security information system

The architecture of a residential complex security information system includes three key subsystems, namely video surveillance, access control, and operator services.

The CCTV subsystem is based on a real-time video recording cameras that are stored on a local DVR or in a cloud storage. The access control subsystem includes access control points that record input and exit, access information that is transmitted to the database for further analysis and monitoring.

The operator's services management subsystem provides integration with suppliers (Internet, security), control by user interface (mobile or web). A description of the main elements of the architecture of a CCTV subsystem (Fig. 8) is shown below.

The camera is responsible for capturing video from different places (inputs, exits, parking, common areas), connects to the DVR and video analytics procedures. The DVR stores the image locally or in the cloud over a certain period and has a channel of transmission of messages from the video camera. The video analytics system processes videos to detect traffic, face recognition, and detect suspicious actions and connect to a DVR to implement access to video materials.

The notification system sends a message to the central control system or user, based on the results of analytical procedures, and is connected to the video analytics system to obtain the results of the analysis. Interface component provides users with access to streaming videos and recorded videos on a real time, it is connected to both a DVR and a video analytics function to implement video interaction with video data.

The central control unit integrates with other subsystems (access control and control system, alarm) for rapid response to incidents. Receives messages from the notification system and

integrates with other components to quickly respond to threats and challenges.

The cameras capture the video flow and transfer it to the DVR. The video analytics system receives video for processing and reveals suspicious actions and transmits the result to the notification system. Users could view the real-time videos or pre-recorded and preserved materials.

The main elements of architecture of the access control subsystem are shown in Fig. 9.

Access control points are physical or electronic devices, in particular card readers, biometric scanners, keyboards for entering personal identification numbers (PINs), low-power Bluetooth labels (BLe) and more. At the same time, these devices are responsible for identifying users before accessing a particular area (entrance to the building, elevator, parking, etc.). The access control server contains a central database that stores information about users, their identifiers, access rights and entry/exit entries. The database receives requests from access control points, checks the user's identification data (card, biometry, PIN) and provides or rejects access. From access control points, data on users' identification to the access control server are transmitted where they are checked. If the identification is successful, the server provides access, and the event information is recorded in the event log. The event log contains records of all inputs and exits, including the time, place, and identification of users. It is connected to the access control server to record information about all access events. The administrator interface is designed to manage users access, adjust the access rules, views of events, etc. It interacts with the access control server to manage settings and monitoring. The user interface provides access through a mobile application or web interface and connected to the access control server to provide users with appropriate features. The system may transmit user entry information to the CCTV subsystem to record video event or module access in case of threats. The administrator interface ensures the function of the subsystem administration, allowing one to change access rules, view events, and analyze information. The user interface gives users a convenient way to access their entrances/exits, as well as the ability to control access. Integration with other subsystems makes it possible to transmit information on access to CCTV subsystem or activate alarm in the event of a threat.

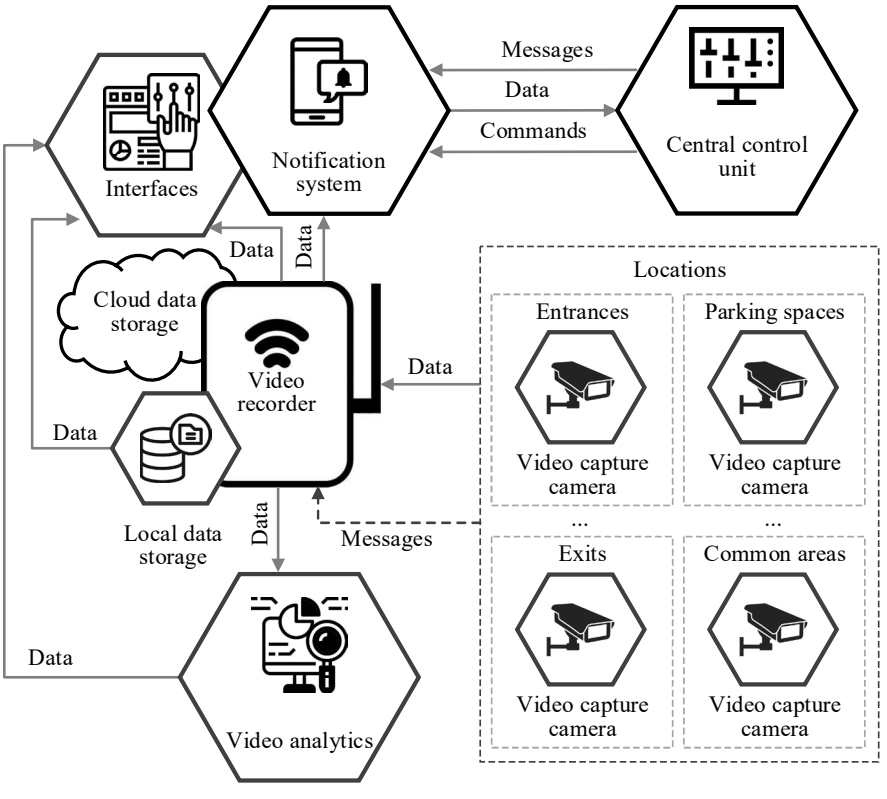

Fig. 8. CCTV subsystem architecture

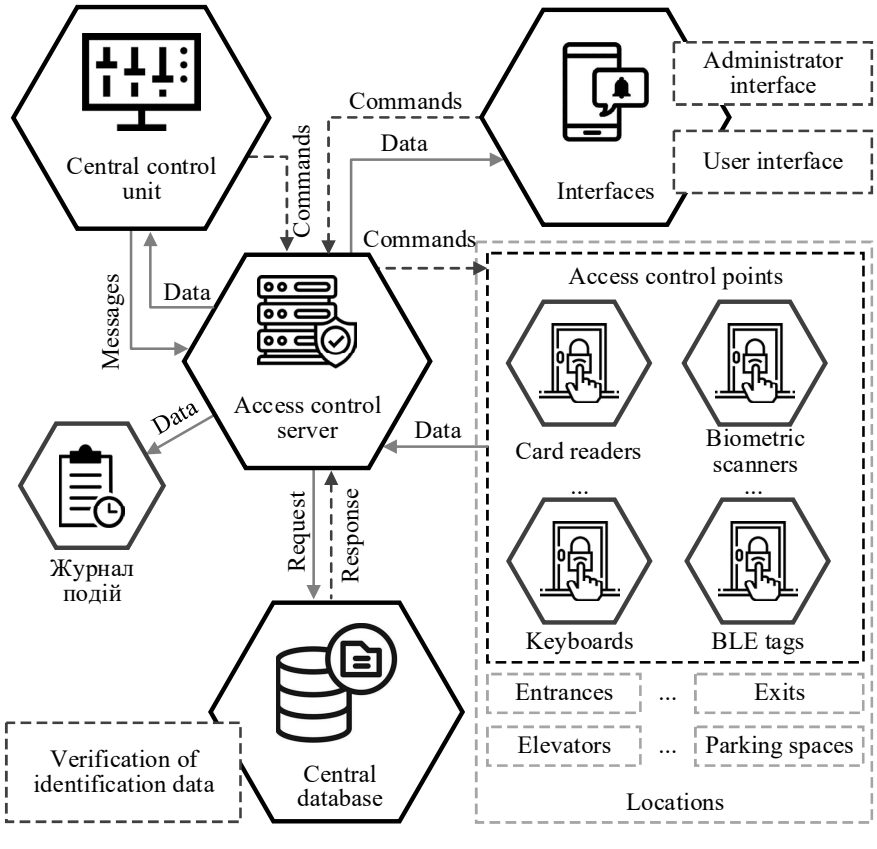

Fig. 9. Access control subsystem architecture

The Services Management Subsystem provides residents with the services of a residential complex, such as Internet services, protection, maintenance of a residential complex, payment of services, and others (Fig. 10).

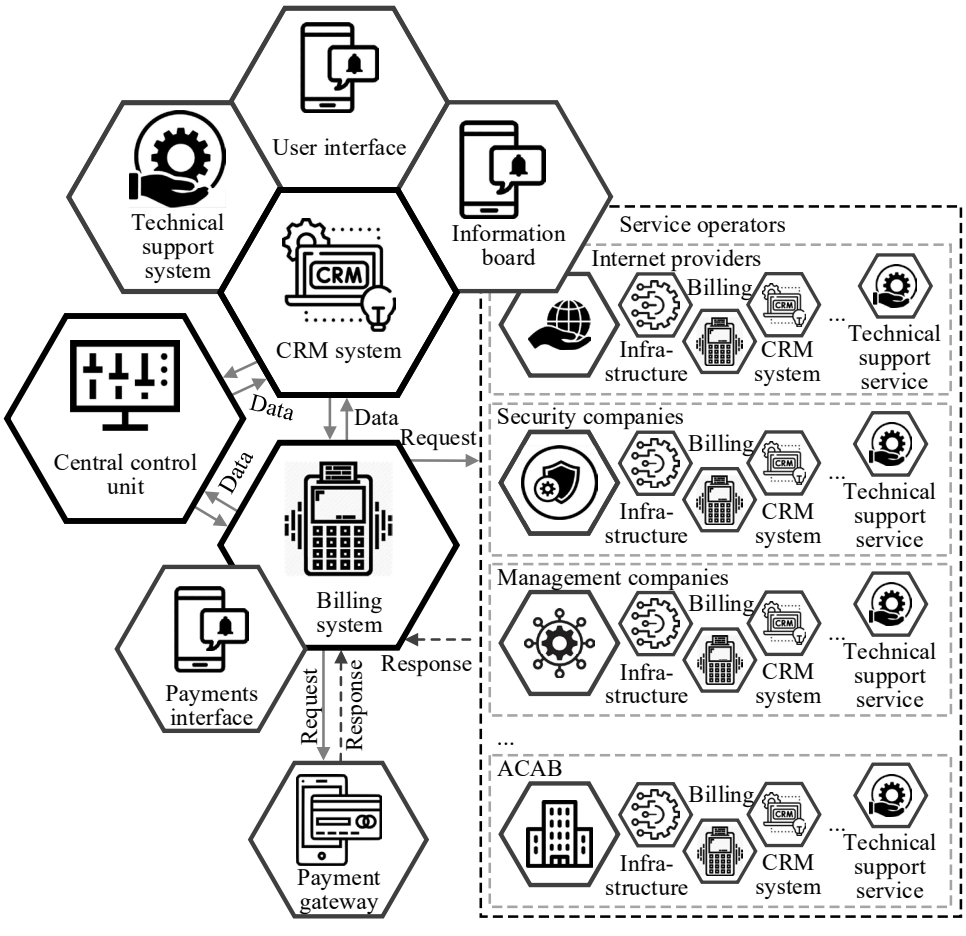

Fig. 10. Architecture of a services management subsystem

The basic elements of the architecture of the Services Management subsystem have been analyzed. Service operators are companies and organizations that provide services to residents: Internet servicemen, security firms, intercom service companies, management companies, associations of co-owners of an apartment building (ACAB). Each operator has its own infrastructure, such as billing systems, the software required for the management of relationships with customers (CRM-systems), technical support services. The billing system is responsible for payment management and accounting for services rendered. Provides interaction with users through an integrated interface for payments. Connected to service operators and interacts with payment gateways to pay for services. The CRM system is used to manage customer relationships, providing access to user information, their subscriptions to services, the history of appeals and technical support. Integrated with other subsystems to support and manage applications from users. The payment gateway is responsible for working out online payments through mobile applications or web interfaces. Connected to the billing system to process payments for residents. Information board is a notification and communication system that informs residents about important events, reports from service operators, residential news, etc. Connected to service operators to automatically send messages through mobile applications or web interfaces.

The user interface includes mobile applications or web interfaces through which users could manage services, pay accounts, receive support, view information about the status of service and receive messages from operators. Integrated with the billing system, CRM, and payment gateways to provide comprehensive service to residents. The technical support system provides support for users on technical issues. Residents could apply for mobile appliances or with a web interface. Integrated with CRM for managing applications and communications with users.

System integration of subsystems. CCTV subsystems, access control and services could work in a single ecosystem using the central control unit that synchronizes their operation. Fig. 11 depicts the integrated representation of components of a security system.

This makes it possible to respond promptly to incidents, automatically control access, and maintain high efficiency of the security information system. Subsystems could be integrated into a single notification system. For example, incidents detected by CCTV subsystem could automatically activate additional functions in the access control subsystem or call maintenance services through the Services Management Subsystem. With the interaction of subsystems, one could automate a number of processes, including opening doors after successful identification using video analytics or automatic creation of technical applications based on cameras and sensors. The simulation modeling of the subsystems has been carried out to evaluate their effectiveness.

The input data of a security information system could be classified as follows: data from IoT devices (video streams from cameras, data from motion sensors, temperature, sound, signals from access control devices (RFID cards, biometric devices), information about the state of infrastructure (e. g., for example, doors, windows), system reaction time, bandwidth, types of events (detection of traffic, access to controlled zones, activation of alarm, change of device status (on/off). Output could be outlined in the following way – notifications for users and personnel (anxieties, statuses), storage of records in the database, generation of analytical reports, commands for performing actions (opening of doors, switch on).

The results obtained have been successfully implemented in the “Astra. Safe RC” software, which is at the stage of implementation and experimental operation.

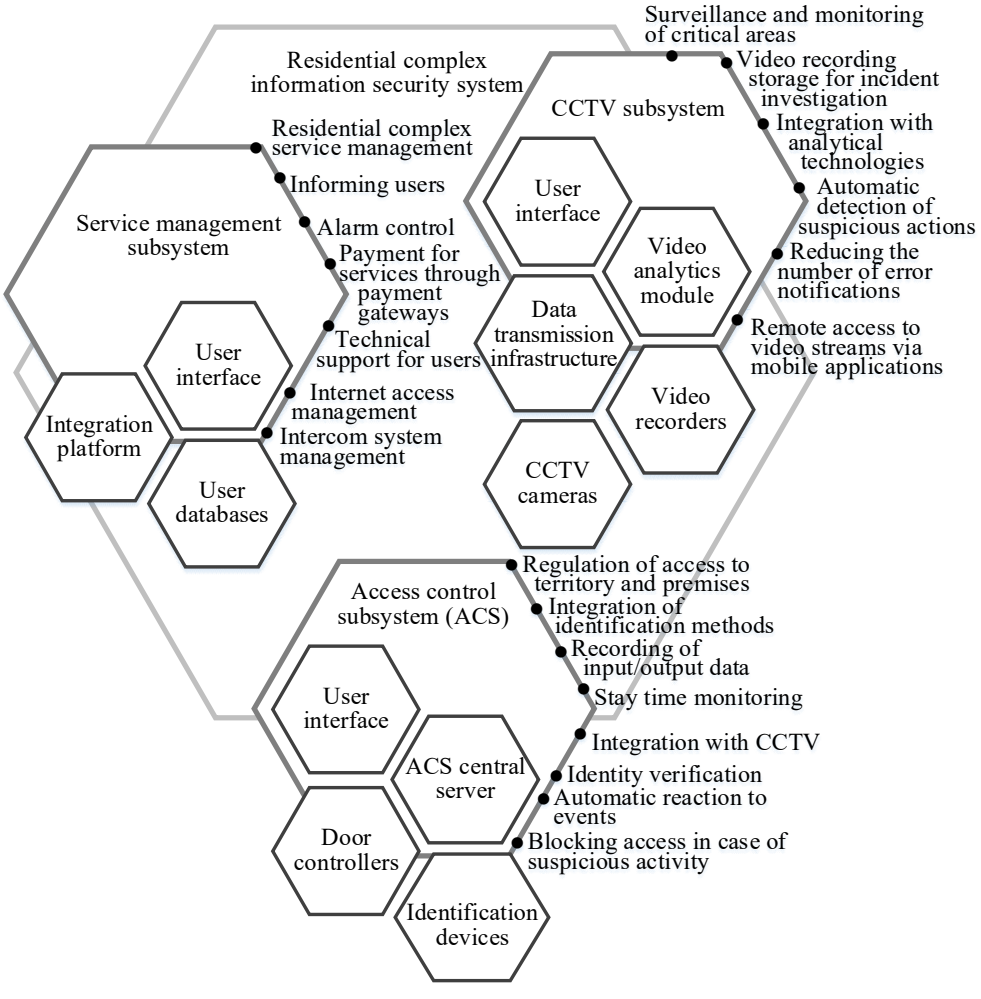

Fig. 11. Integrated representation of components in an information system for residential complex security

The specified subsystems are part of the architecture for a security information system. They provide the functionality that is needed to achieve a wide range of system goals. Integration of CCTV subsystems, access control, and service management is a key factor in designing an effective and reliable residential quarter information system.

A hybrid infrastructure, which combines local servers, cloud services, and developed network architecture, was used to deploy the information system with situational awareness in the residential complex. Involvement of an ACAB internet service provider makes it possible to effectively use existing infrastructure, minimizing the cost of implementing and maintaining the information system. Implementation of the information system for residential complex security on the functional field of the largest Lviv regional Internet service provider Astra has added to it the following advantages: the use of the provider's cable infrastructure in RC for fast and rational deployment, the use of server infrastructure for the DevOps methodology for monitoring, protecting from cyberattacks, and operational scaling.

This will formalize approaches to designing the structure and architecture of an information system and to providing a comprehensive approach to information protection and management of security processes within residential complexes.

6. Discussion of results based on constructing the structure and architecture of a security information system

On the basis of our analysis, it was found that most existing security systems have some restrictions on providing comprehensive situational awareness, adaptability, and integration with the technologies of the Internet of Things.

The proposed system has been designed taking into account the benefits of systems of this type for the purpose of better analysis and response to situations that arise in residential complexes, in real time (Table 1). Unlike a model of situational awareness, given in work [1], intelligent agents have been used to support decision-making and analysis of situations. They are able to act autonomously in the environment, making decisions based on the data obtained and performing the task without human intervention. Intelligent agents track object parameters based on data obtained from a sensor or group of sensors, interpreting them as parameters of ontology objects.

It is established that conventional residential safety systems often do not provide effective exchange of data between different components, which complicates centralized control and reduces the speed of response to potential threats. In order to avoid this, the main components that must be integrated into a complex system are intelligent agents,

the central control unit, internal software, and IT network services (Fig. 5). It is the formalization (1) of the systemic combination of these components that helps improve the implementation of monitoring, control, and automated data processing functions in the system, as opposed to previous studies [11, 12].

The structure of the designed system includes the integration of intelligent agents, server services, the central control unit, sensors, and knowledge bases (Fig. 1). This allows the system to interact effectively with all the components and to ensure the processing of information in real time. Intelligent agents (1) and internal software services (2) implement the functions of automated decision making and data processing, and the central control unit (3) controls all processes and performs centralized monitoring. Thanks to the structure that combines these components, the information system is able to respond promptly to threats and effectively manage security functions, which increases the overall level of safety of the residential complex.

The role of intelligent agents (Fig. 1) in the information system is to perform autonomous functions of collecting and analyzing data from sensors, which makes it possible to provide situational awareness at the local level, which distinguishes the designed structure from previous work [13]. Internal software services (Fig. 2) perform computing tasks, such as templates and machine learning, which allows the system to increase the accuracy of threats. The central control unit (Fig. 3) aggregates data from agents and internal services, which makes it possible to create a general picture of the situation in the complex and respond to potential threats in a timely manner. This structure (4) increases the level of situational awareness and allows the system to adapt to changes in the environment through the interaction of elements (5)–(7).

The designed architecture (Fig. 7) includes the main subsystems: video surveillance, access control, and operator services, unlike a five-level one [13]. Formally, the architecture of the residential complex security information system is represented with a tuple (8). The CCTV subsystem (9) provides the collection and processing of video data, which makes it possible to identify abnormal events and ensure the safety of the perimeter. The access control subsystem (10) is responsible for identifying and checking the persons who are included and out of the residential complex. The operator's services management subsystem (11) provides communication between the information system and operators to respond to real-time events. This architecture makes it possible to construct a single security management system with clearly separated functions and powers (Fig. 6), unlike [4].

The system as a whole (Fig. 6) and each of the subsystems has its own functional features that form individual groups of elements and connections between them. CCTV subsystem (Fig. 8) performs real-time monitoring functions and provides video archives. The access control subsystem (Fig. 9) provides automated access and accounting of visits, and the operator's services management subsystem (Fig. 10) performs requests and responds to the incident reports. It is established that the effective functioning of the system depends on the coordinated operation of these subsystems, and the distribution of their functions and interconnections ensure the flexibility and adaptability of the system to the specific tasks of the residential complex (12).

The formalization of structure (4) and architecture (8) of the residential complex information system provides a comprehensive approach to the formation of these concepts and provides their characteristic features. The integration of intelligent agents, internal services, the central control unit, and IoT networks allows the system to perform the basic functions of protection, monitoring, analysis, and response to real-time threats.

The success of our research is due to the development of a security information system based on situational awareness, using innovative approaches. The security information system achieves high levels of flexibility, adaptability, throughput, and integration of subsystems into a single vast IoT network. It has a number of significant advantages, among which the following should be noted the possibility of combining and flexible distribution of considerations between intelligent agents and server services, adapting to diverse computing needs when performing a wide range of tasks.

In practice, the results of our work will create an effective intelligent security system. It could respond promptly to threats, provide automated access control, real-time monitoring, and processing data on events to maintain a safe environment.

The restriction of the application of the proposed solutions relate to the need to constantly replenish the knowledge base with the descriptions of situations used for comparative analysis and decision-making in the face of a threat in real time.

Continuation of scientific research is the area of forming a methodological basis for designing a spectrum of security information systems using the concept of situational awareness. They are intended for use in multi-apartment buildings, residential complexes, quarters, micro-districts, neighborhoods, and cities in general. At the same time, a significant expansion of the spectrum of types of situational awareness in security information systems is expected, which would cover a significantly larger set of security profiles, which could make it possible to scale the designed information system to the wider environment indicated above.

7. Conclusions

1. The structure of a security information system has been designed, which combines key components into a single adaptive network, and its basis is an IoT network that provides integration of sensors and other devices with the central control unit. Intelligent agents on the basis of knowledge base implement the processes of analysis, autonomy of decision-making. They make it possible to perform local data processing and interact with other nodes of the system autonomously. The proposed structure takes into account the possibility of dynamic scaling and updating of the IoT network components. The uniqueness of the developed structure is the integration of intelligent agents with the central control unit, which provides not only centralized but also decentralized process management. The system works using situational-oriented conceptual models of specific situations that are obtained from the knowledge base using the similarity factor of contexts. Thanks to this approach, information system with situational awareness is able to model and analyze the state of the environment in a real time, identify situations, make decisions, and act according to them. The system maintains a continuous learning process of reconciling the

projected data with sensors. This result is predetermined by the need to increase the autonomy of the system and ensure its scalability for use in various residential complexes.

2. It has been revealed that intelligent agents effectively reduce the load on the central control unit, performing the primary analysis of data and making decisions in real time. These elements of the structure make it possible to combine different types of tasks in the information system, taking into account the situation and dynamically distributing the computing load between agents and services. Internal software services contribute to the integration of all components and automation of security processes. Centralized solutions are executed faster thanks to the pre-filtration by these agents. Internal software makes it possible to flexibly adjust the behavior of subsystems. In most known security systems, the focus is only on centralized management, while the designed information system combines the benefits of centralized and decentralized approaches. This is explained by the need to reduce delays in decision making and increase the resistance of the system to the failures of its individual components.

3. An architecture has been proposed that combines video surveillance subsystems, access control, and operator services using a single data processing center. The architecture takes into account the compatibility of subsystems and their integration into the IoT network. The priority of processing critical events is ensured, which reduces the response time. Such integration of subsystems makes it possible to fully and systematically reflect a holistic picture of the security situation to the operator. At the same time, the designed architecture makes it possible to simultaneously manage subsystems in real time, which was not always implemented in known systems because of their compatibility restrictions. The result has been achieved by standardizing data transmission protocols and IoT-network integration with appropriate control algorithms.

4. Classification of subsystems elements has been performed and existing relationships between them have been analyzed. The use of analytical algorithms and cloud services provides opportunities to provide operational control, monitoring, threat analysis, and prompt response to potential incidents. The evaluation of efficiency of the subsystems work reported that the average subsystem reaction time was 0.7 seconds, and their throughput included the ability to process up to 100 events per minute. An approach to determining critical relationships between elements has been devised, which makes it possible to optimize the work of the entire system. Most approaches known at present do not take into account the variants of sets of relationships, focusing solely on individual aspects. Our result is explained by the use of a systematic approach to modeling processes that cover full sets of options for interaction of functional subsystems.

Conflicts of interest

The authors declare that they have no conflicts of interest in relation to the current study, including financial, personal, authorship, or any other, that could affect the study, as well as the results reported in this paper.

Funding

The study was conducted without financial support.

Data availability

All data are available, either in numerical or graphical form, in the main text of the manuscript.

Use of artificial intelligence

The authors confirm that they did not use artificial intelligence technologies when creating the current work.

References

1. Munir, A., Aved, A., Blasch, E. (2022). Situational Awareness: Techniques, Challenges, and Prospects. AI, 3 (1), 55–77. https://doi.org/10.3390/ai3010005
2. Endsley, M. R. (1988). Design and Evaluation for Situation Awareness Enhancement. Proceedings of the Human Factors Society Annual Meeting, 32 (2), 97–101. https://doi.org/10.1177/154193128803200221
3. Kwok, K., Virdi, S. (2022). AI-Based Situation Awareness Assessment. Journal of Physics: Conference Series, 2311 (1), 012011. https://doi.org/10.1088/1742-6596/2311/1/012011
4. Parker, J. (2023). What is information system architecture? Architecture. Available at: https://www.architecturemaker.com/what-is-information-system-architecture/
5. Golnabi, H. (2023). Smart sensors development and applications. Proceeding of Flexible Automation and Integrated Manufacturing 1998, 635–643. https://doi.org/10.1615/faim1998.570
6. Duda, O., Kochan, V., Kunanets, N., Matsiuk, O., Pasichnyk, V., Sachenko, A., Pytlenko, T. (2019). Data Processing in IoT for Smart City Systems. 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), 96–99. https://doi.org/10.1109/idaacs.2019.8924262
7. Tolkachov, M., Dzheniuk, N., Yevseiev, S., Lysetskyi, Y., Shulha, V., Grod, I. et al. (2024). Development of a method for protecting information resources in a corporate network by segmenting traffic. Eastern-European Journal of Enterprise Technologies, 5 (9 (131)), 63–78. https://doi.org/10.15587/1729-4061.2024.313158
8. Li, Y., Che, Q., Wang, F., Zhang, H., Wang, W., Jiang, Y. (2024). A Method for Security Traffic Patrolling Based on Structural Coordinated Proximal Policy Optimization. Computer Supported Cooperative Work and Social Computing, 62–76. https://doi.org/10.1007/978-981-99-9640-7_5
9. Blakely, B., Horsthemke, W., Harkness, D., Evans, N. (2023). Deployment and Operation. Autonomous Intelligent Cyber Defense Agent (AICA), 295–310. https://doi.org/10.1007/978-3-031-29269-9_14

10. Kaldeli, E., Warriach, E. U., Lazovik, A., Aiello, M. (2013). Coordinating the web of services for a smart home. ACM Transactions on the Web, 7 (2), 1–40. https://doi.org/10.1145/2460383.2460389
11. Barcelo, M., Correa, A., Llorca, J., Tulino, A. M., Vicario, J. L., Morell, A. (2016). IoT-Cloud Service Optimization in Next Generation Smart Environments. IEEE Journal on Selected Areas in Communications, 34 (12), 4077–4090. https://doi.org/10.1109/jsac.2016.2621398
12. Mocrii, D., Chen, Y., Musilek, P. (2018). IoT-based smart homes: A review of system architecture, software, communications, privacy and security. Internet of Things, 1-2, 81–98. https://doi.org/10.1016/j.iot.2018.08.009
13. Hassan, S. A. Z., Eassa, A. M. (2022). A Proposed Architecture for Smart Home Systems Based on IoT, Context-awareness and Cloud Computing. International Journal of Advanced Computer Science and Applications, 13 (6). https://doi.org/10.14569/ijacsa.2022.0130612
14. Burov, Y., Zhovnir, Y., Zakharya, O. (2024). The vision and implementation of intelligent security system. Herald of Khmelnytskyi National University. Technical Sciences, 341 (5), 497–509. https://doi.org/10.31891/2307-5732-2024-341-5-72