Universal security platform for intelligent cyber-physical technology of regional carbon dioxide monitoring*

Valerii Dudykevych[1,*,†], Halyna Mykytyn[1,†], Sviatoslav Borduliak[1,†], and Yaroslav Fur[1,†]

[1] *Lviv Polytechnic National University, 12 Stepana Bandery str., 79000 Lviv, Ukraine*

Abstract

The concept of Industry 4.0 and Ukraine's Cybersecurity Strategy, in their respective vectors, foresee the development of methodological approaches for the application of secure intelligent technologies, particularly for the functional support of the emergency monitoring segment, including greenhouse gas emissions into the regional ecosystems of Ukraine. This study explores the aspects of developing an intelligent cyber-physical technology (ICPT) for monitoring carbon dioxide parameters in the air ecosystem based on a universal platform: "ICPT architecture—integrated security model—comprehensive security systems." A multi-level ICPT architecture is proposed, enabling the selection of carbon dioxide concentration under the influence of both anthropogenic and natural factors on the regional air ecosystem within the framework of "control—processing—management." This architecture serves as the foundation for creating an integrated multi-level security model for ICPT. The functional architecture of the multi-level ICPT is deployed at the technology levels: physical space (PS), communication environment (CE), and cybernetic space (CS). Based on the integrated security model and the "object—threat—protection" concept, comprehensive security systems (CSS) have been developed for the ICPT levels—PS, CE, and CS—under the impact of both targeted and random threats. A software implementation of cryptographic protection for the ICPT cybernetic space database has been developed using the symmetric block encryption algorithm "Kalyna" in a programming language.

Keywords

intelligence, emergencies, monitoring, carbon dioxide, regional ecosystem, cybersecurity, intelligent cyber-physical technology, integrated model, comprehensive security system, database encryption

1. Introduction

Today, approaches to solving the problem of secure intelligence integration of Ukraine's infrastructure objects, particularly critical ones under global challenges, are actively developing. The relevance of the cybersecurity vector is highlighted in the Industry 4.0 Concept, the COP 29 Climate Summit (September 2024, Azerbaijan, Baku), and the Ninth Framework Programme "Horizon Europe" (2021–2027), particularly in the implementation of advanced science technologies based on systemic and synergistic principles. An effective tool for addressing the problem of secure intelligence integration of societal infrastructure objects within the framework of the Cybersecurity Strategy of Ukraine (2021–2025) is intelligent cyber-physical technologies (ICPTs) and their comprehensive security systems (CSSs) [1].

Cyber-physical technologies, as one of the main tools for monitoring carbon dioxide within emergency environments in a region, are developing along the vectors of architecture and cybersecurity. Let us consider some trends in Ukraine and internationally. The application of intelligent cyber-physical technologies within the Industry 4.0 Concept is an emerging field, particularly involving artificial intelligence elements in industrial ICPTs for decision-making in domain-specific societal areas [2–5]. The study [6] explores models and methods for information security based on a multi-loop approach to the secure functioning of information resources in ICPTs. To ensure confidentiality and data integrity protection in ICPTs, the author [7] outlines

* *CPITS-II 2025: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, October 26, 2025, Kyiv, Ukraine*

* Corresponding author.

† These authors contributed equally.

valerii.b.dudykevych@lpnu.ua (V. Dudykevych); halyna.v.mykytyn@lpnu.ua (H. Mykytyn); sviatoslav.borduliak.mkbst.2024@lpnu.ua (S. Borduliak); yaroslav.fur.mkbas.2023@lpnu.ua (Y. Fur)

0000-0001-8827-9920 (V. Dudykevych); 0000-0003-4275-8285 (H. Mykytyn); 0009-0007-2076-9297 (S. Borduliak); 0009-0006-1867-1146 (Y. Fur)

requirements for the use of cryptographic tools. The study [8] presents the direction of development of cryptographic tools to ensure data security at the level of one of the segments—a pseudorandom bit sequence generator with increased cryptographic security, which provides effective counteraction to cybercrime in the subject areas of society's infrastructure [9].

Today, the processes of interconnecting the architecture and security of cyber-physical technologies are unfolding, particularly at the conceptual level in accordance with the paradigm "multi-level ICPT—multi-level security" [10, 11], as well as models, methodology and an integrated information technology security system [12, 13], which is being implemented in the field of safe operation of cyber-physical power systems [14, 15]. Further advancements are being made in ICPT architecture at the level of integrating computation, networking, and physical processes, as well as their effective interdisciplinary application [16, 17]. The monograph [18] considers the application of situational management methods to ensure the safe functioning of socio-cyber-physical systems, logical and transformational rules that are the basis for building a situational cybersecurity management system. In the area of information systems infrastructure security, a methodology for detecting cybercrime using decoys based on blockchain technology is proposed in [19]. In line with the vectors of Industry 4.0 tasks, the authors of [20] present a universal platform for the secure intellectualisation of society's infrastructure based on the concept of cyber-physical systems security and the system security model of the three-tiered architecture of the Internet of Things.

The objective of this study is to develop a security methodology for intelligent cyber-physical technology (ICPT) for monitoring carbon dioxide levels in the air ecosystem of a region under the influence of technogenic and natural factors. This methodology follows the structure: "ICPT architecture—multi-level security model—comprehensive security systems (CSSs)", implementing a constructive algorithm for secure functioning based on the "object—threat—protection" concept.

2. Architecture of the Multi-Level ICPT for Monitoring Carbon Dioxide in the Regional Ecosystem

In the context of the Emergency Monitoring Regulation [21], which addresses emergencies arising from negative technogenic factors (such as greenhouse gas emissions, including carbon dioxide; hazardous substances, including radioactive materials; accidents in power systems; emergency situations in the oil and gas industry, etc.) and natural factors (such as geophysical, meteorological, and medical-biological events), the application of effective intelligent technologies in the "control—processing—management" domain is highly relevant. Among these technologies, multi-level cyber-physical technologies (CPTs) play a key role. Figure 1 presents the functional structure of a three-level ICPT for air environment monitoring, focusing on carbon dioxide content at the following levels: Physical Space (PS)—Sensors for collecting information on the state of the regional air ecosystem.

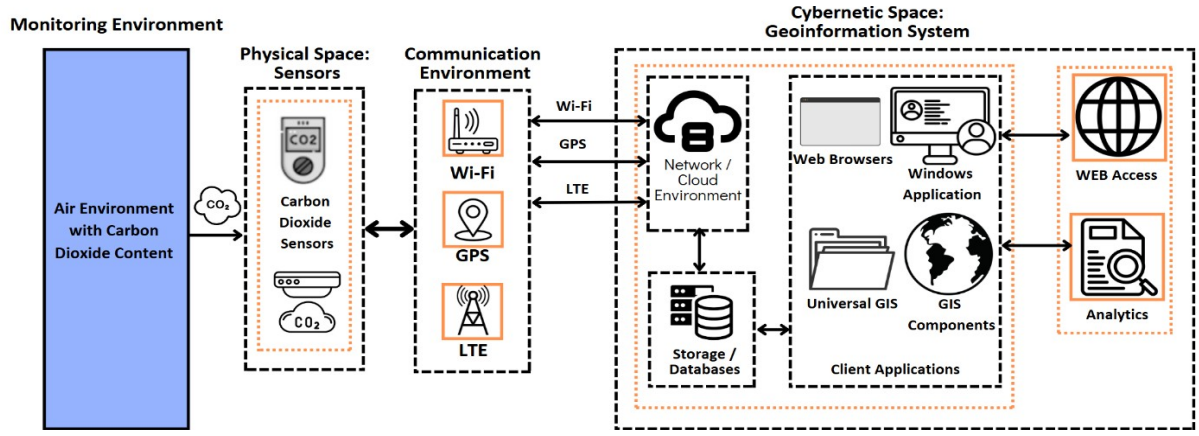

Figure 1: Architecture of the Intelligent Multi-Level Cyber-Physical Technology for Monitoring Carbon Dioxide in the Regional Ecosystem

Communication Environment (CE)—Wireless data exchange networks (Wi-Fi, GPS, LTE). Cybernetic Space (CS)—A Geoinformation System (GIS) integrated with web applications and an analytical center.

3. Multi-Level Security of the Intelligent Cyber-Physical Technology for Carbon Dioxide Monitoring

In order to ensure the integrity of the security of the three-level ICPT for monitoring carbon dioxide in the region's ecosystem, the following are proposed: an integrated model of multi-level security of the intelligent cyber-physical technology for monitoring carbon dioxide in the region's air ecosystem; integrated security systems for the physical space, communication environment, and cyberspace of the ICPT, which provide methods and means of protection in the event of a complex of random and targeted threats.

3.1. Integral Model of the Intelligent Cyber-Physical Technology for Carbon Dioxide Monitoring

The ICPT for CO_2 monitoring adopts a mandatory (multi-level) security policy, which offers a higher level of protection compared to discretionary and role-based security policies. Key Features of the Mandatory Security Policy for ICPT in Emergency Situations: (1) Definiteness of the confidentiality lattice of information; assigning each system object the corresponding level of confidentiality based on the value of information in relation to the object; (2) Satisfaction of identification requirements for all subjects and objects of the system; (3) Implementation of an algorithm to prevent information leakage between objects with different access levels.

Mandatory access control ensures adherence to a set of security rules regulating user/system access to specific resources. The mandatory security policy of the ICP technology enables: assessment of threats and risks at the vulnerability identification level; implementation of access and authentication policies at the level of establishing defined rules, as well as user authentication mechanisms; data protection at the level of developing security strategies for confidential information using encryption tools; staff training at the level of conducting relevant training sessions; monitoring and responding to incidents at the level of implementing event tracking systems in the system [22]. The multi-level security model of the ICPT is illustrated in Figure 3.

3.2. Integrated Security System for the Physical Space of ICP Technology: Data Collection Sensors—Threats—Protection Technologies

Concentration Monitoring Sensors are installed at locations for monitoring greenhouse gas emissions and are equipped with micro controllers for data processing, batteries, GPS modules, and LTE system antennas for data transmission. The functional process of data collection, processing, and transmission of carbon dioxide monitoring in the air ecosystem is depicted in Figure 2.

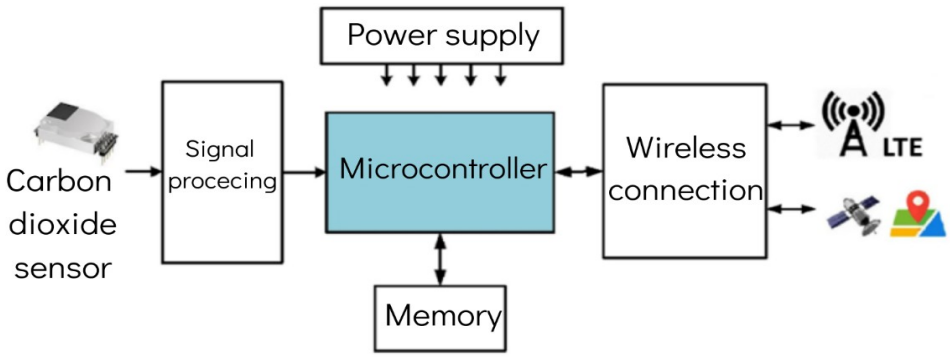

Figure 2: Data Collection, Processing, and Transmission Process for Carbon Dioxide Monitoring in the Region's Ecosystem

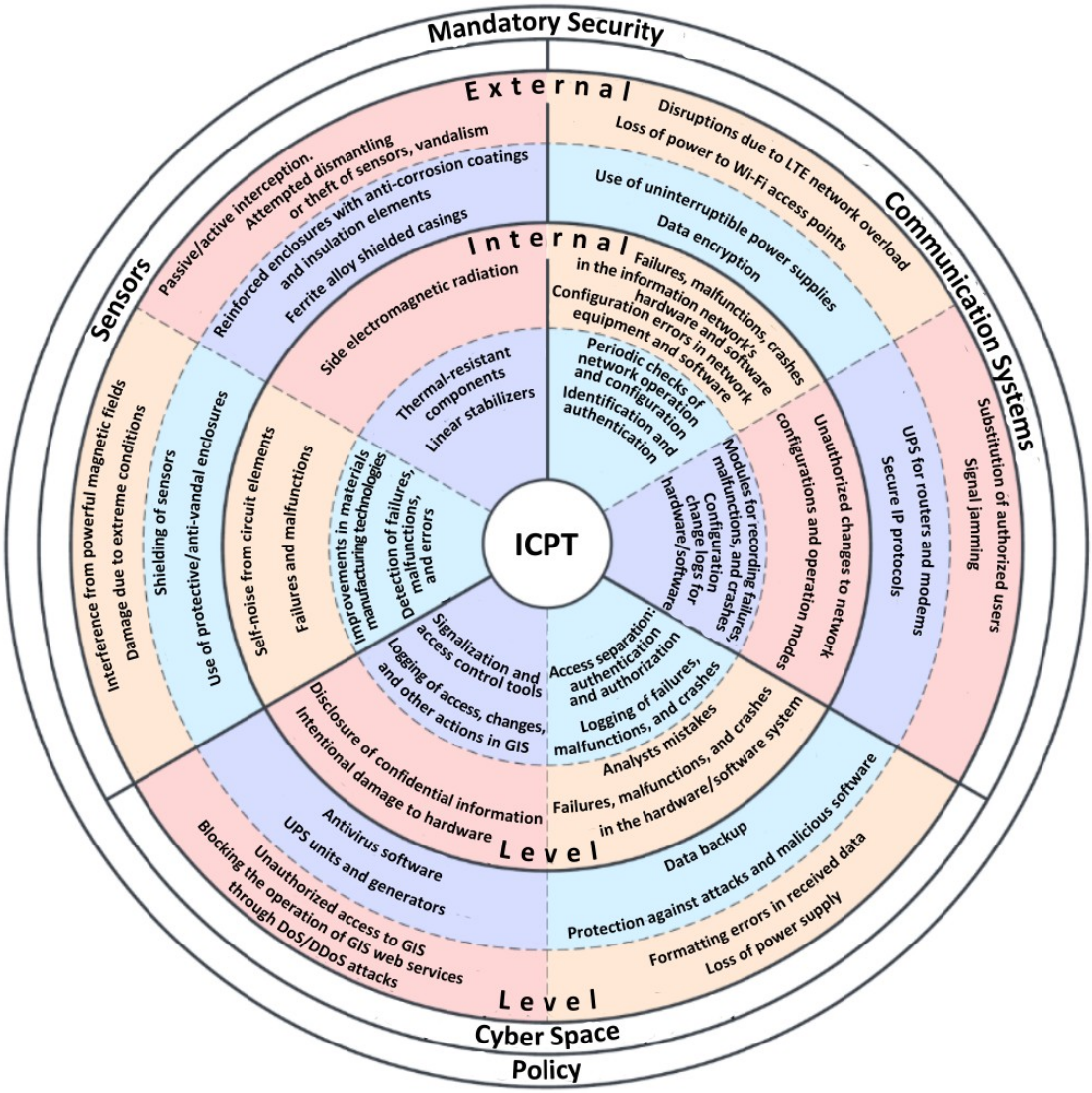

Figure 3: Integrated Model of Multi-Level Security for the Intelligent Cyber-Physical Technology for Monitoring Carbon Dioxide in the Air Ecosystem of the Region: Threats—Protection Technologies: —Accidental threats, —Targeted threats, —Protection methods, —Protection tools

In practice, the following models of Infrared (NDIR) analyzers for monitoring carbon dioxide concentration in the region's ecosystem are effectively used: RK300-03A (Figure 3a) and RK300-03B (Figure 3b) CO2 Concentration Sensor [23]; CM1106SL-NS Super Low Power CO2 Sensor Module (Figure 3c) [24].

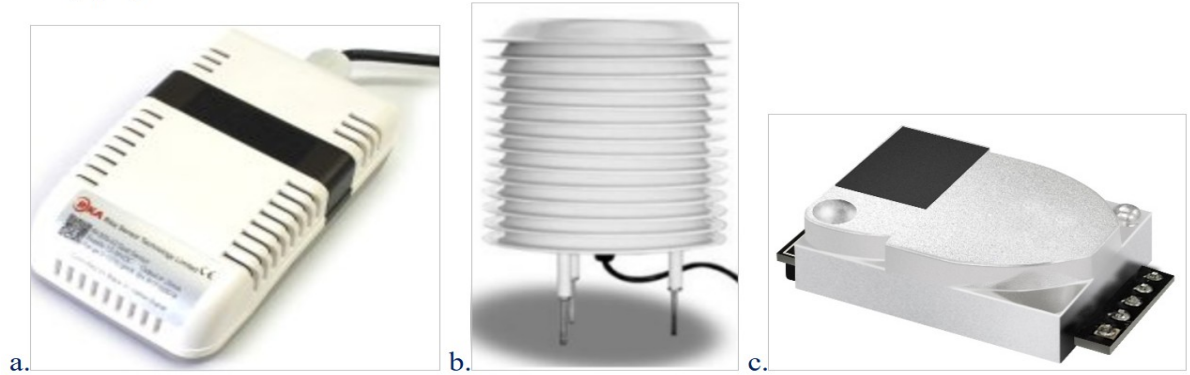

Figure 4: Carbon Dioxide Concentration Analyzers: a—RK300-03A; b—RK300-03B; c—CM1106SL-NS

The RK300-03 model has two versions: for indoor installation—RK300-03A; for outdoor installation —RK300-03B. The CM1106SL-NS model is a separate small electronic module for measuring carbon dioxide concentration, installed in a protective housing, and allows continuous monitoring at remote locations in real-time mode. The main characteristics of the carbon dioxide analyzers are provided in Table 1. The STM32L072RBT6 micro controller performs: signal analysis from the sensor, data storage, and in real-time mode, uses the LTE module with an antenna to transmit the accumulated data to the cyber space of the ICP technology.

Table 1
Main Characteristics of Carbon Dioxide Concentration Analyzers

Characteristics	RK300-03	CM1106SL-NS
Measurement Range, ppm	0-5000, 0-10000	0-5000
Accuracy	±50 ppm +2% of the value	±50 ppm +5% of the value
Power Consumption	<0.25 watts	0.32 or 0.16 milliwatts
Response Time/Measurement Cycle	<20 seconds	1 or 2 minutes

Let's consider the integrated security system of the intellectual cyber-physical technology at the physical space level, the components of which are sensors (Table 2).

Table 2
Integrated Security System of the Physical Space of ICTF: Sensors—Threats—Protection Technologies

Purpose: Data selection security	**ICTF Segment: Physical space**	**Threats**	**Security Technologies – Security Profiles (confidentiality, integrity, availability)**	
			Methods of Protection	**Protection Tools**
Secure CO2 concentration selection in the ecosystem of the air environment of the region	Sensors embedded in various physical objects/ecosystems (RK300-03A, RK300-03B, and CM1106SL-NS); Special sensors embedded in devices; MEMS sensors	*Random:* Human error as part of the system Structural, algorithmic, software errors Failures and malfunctions Interference in communication lines Line loadings Noise from circuit elements Temperature dependencies Wear and tear Damage due to	Detection and diagnosis of failures, algorithm faults, program errors, human mistakes Improvement of material manufacturing technology Use of protective housings Electromagnetic shielding of sensors	Line stabilizers Thermostat elements Housings with anti-corrosion coating and insulating elements Shielded enclosures made of ferrite alloys

	extreme weather conditions (hail, freezing) Interference due to the influence of powerful magnetic fields (near industrial objects)		
	Targeted threats:		
	Access to user terminals, administration, control Passive/active interception Side electromagnetic radiation of information Attempt of physical disassembly or theft of the sensor, vandalism	Access control to terminals Access control to the installation of communication lines and equipment Identification and authentication Protection from side radiation and inductions Equipping devices with motion detection systems Use of anti-vandal housings	Identifiers Access control devices Devices that protect from side radiation Built-in tilt or motion sensors that transmit alarm signals Reinforced metal housings and shock sensors

3.3. Integrated Security System of the Communication Environment of ICTF: Wireless Communication Technologies—Threats—Protection Technologies

In the ICTF monitoring system of carbon dioxide in the region's ecosystem, several wireless communication technologies are used for data transmission: LTE technology for transmitting monitoring data from sensors to the cybernetic space of ICTF; GPS technology for precise location determination of each sensor; Wi-Fi technology for wireless data transmission within the analytical center, as well as a possible replacement for LTE technology in certain cases.

The advantages of LTE technology include availability, reliability, and the ability to function over long distances. This technology is characterized by high bandwidth and low latency, which is essential for real-time monitoring, such as tracking spikes in carbon dioxide concentration in city ecosystems during peak hours.

GPS is a satellite navigation system that provides information about the location of the carbon dioxide monitoring sensor in the air ecosystem and the time, under any weather conditions, anywhere on Earth where there is an unobstructed line of sight to four or more GPS satellites (the full constellation consists of 24 satellites). GPS system modules are used in carbon dioxide measurement sensors. Recording the exact location of each sensor along with its monitoring data provides a GIS that can automatically generate a 3D map of carbon dioxide concentration in the region's ecosystem.

Wi-Fi is a standard for wireless local area network (LAN) connections that enables communication between various devices over short distances (up to several dozen meters) based on the IEEE 802.11 standard. Among the main advantages of Wi-Fi technology are mobility,

convenience, transmission speed, and energy efficiency. Wi-Fi technology allows network deployment without the need for wiring, simplifying and speeding up the installation and modification process. It also provides Internet access anywhere with coverage, which is especially convenient for mobile devices, and is effectively used to support the operation of Internet of Things devices.

Let's consider the integrated security system of wireless technologies at the communication environment level of ICTF (Table 3).

Table 3
Integrated Security System of the Communication Environment of ICTF: Wireless Communication Technologies—Threats—Protection Technologies

Purpose: Data selection security	**ICTF Segment: Communication environment**	**Threats**	**Security Technologies – Security Profiles (confidentiality, integrity, availability)**	
			Methods of Protection	**Protection Tools**
Secure data exchange in ICTF	Wireless communication technologies: LTE GPS Wi-Fi	*Random:*		
		Incorrect use of local network resources Errors in the administration and configuration of network equipment and software Failures, malfunctions, system crashes of hardware and software	Partitioning available resources into time intervals Increasing network bandwidth Conducting periodic checks on operational modes and network configuration Logging failures, malfunctions, system crashes Functional control of hardware and software in IM (K)	Network resource usage control system Network equipment/software configuration change log Sensors Centralized information collection devices Modules for logging failures, malfunctions, and system crashes
		Targeted threats:		
		Analysis and interception of traffic circulating in the network Unauthorized modification of network configuration and operational modes Targeted	Avoid transmitting confidential information over unsecured communication channels Modulation, signal manipulation Conduct periodic checks on operational modes,	Cryptographic transformation tools Secure IP protocols Modulators, demodulators Identifiers Checkpoints Signaling devices

	violation of information integrity, authenticity, or availability in the network Impersonation of an authorized user (Man-in-the-Middle attack) Signal jamming	restrict access to network equipment and software User and network parameter identification and authentication Data encryption Data hashing Data backup Digital electronic signature method Switching to backup communication channels	Key and code locks Hash functions, hash tables Tools for implementing electronic digital signatures Digital certificates of equipment Modules supporting NB-IoT, LTE/LTE-M, or Wi-Fi as backups

3.4. Integrated Security System of the Cybernetic Space of ICTF: Geoinformation System—Threats—Protection Technologies

The Geoinformation System for Monitoring Carbon Dioxide in the Air Ecosystem of the Region is the core of the ICTF. It is a complex decision-support system that: consolidates the functions of organizing, storing, analyzing, and visualizing regional geographic data; integrates hardware and software, data, and functions. It physically consists of databases, data storage, and workstations for analysts with specialized software (SW), all connected in a local network. The GIS is built on the basis of professional software packages, such as ArcGIS, and the complete life cycle of processing monitoring data covers the following stages:

The Geoinformation System for Monitoring Carbon Dioxide in the Air Ecosystem of the Region in the cybernetic space of ICTF operates as follows [25]:

1. Data Collection/Selection: The functioning of GIS in the cybernetic space of ICTF focuses on: gathering spatial and attribute data from existing sources (datasets, satellite imagery, etc.); selecting data from the physical space (sensors of ICTF).
2. Data Storage: The GIS of ICTF uses databases and data storage systems to store and manage the collected data. These systems organize data for efficient search, updates, and sharing. Relational or spatial databases, such as PostgreSQL/PostGIS or Esri's File Geodatabase, are used. File formats include Shapefiles, GeoTIFF, KML, GeoJSON, etc.
3. Data Processing and Management: Raw data often requires pre-processing before use, such as cleaning (removing errors or inconsistencies), projection and transformation (bringing data into a unified coordinate system), and integration (combining multiple datasets and creating a unified representation). Computer programs like ArcGIS are used for this and subsequent stages.
4. Spatial Data Analysis: GIS of ICTF allows spatial analysis of prepared data using algorithms and tools: layer overlay (combining layers to identify relationships and correlations), proximity analysis (finding the nearest objects, e.g., locating the nearest CO2 sensor to a specific facility), and terrain and elevation analysis (using 3D data to analyze the impact of terrain on the distribution of carbon dioxide, or the dynamics of CO2 distribution in dense urban areas).

5. Data Visualization: GIS of ICTF visually represents data through maps, graphs, and 3D models. These visualizations help analysts and users understand spatial relationships and patterns, make informed decisions, and generate reports using interactive or printed maps.
6. Decision Support: The GIS of ICTF for carbon dioxide emission monitoring in the region serves as the main tool for data processing, analysis, and, based on this, supporting decision-making related to managing greenhouse gases, complying with established plans and agreements, and preventing emergencies in the region.

Let's consider the comprehensive security system of the ICTF at the level of the cybernetic space, the main component of which is the GIS (Table 4).

Table 4
Comprehensive Security System of the ICTF Cybernetic Space: Geographic Information System – Threats—Security Technologies

Purpose: Security of processing, analysis, storage, and decision-making	**Segment of ICTS: Cybernetic Space**	**Threats**	**Security Technologies – Security Profiles (confidentiality, integrity, availability)**	
			Methods of Protection	**Protection Tools**
Processing of monitoring data, analysis, storage, and decision support for management.	Geographic Information System for data processing, analysis, storage, and decision-making for management: Databases, data storage Cloud environment Hardware and software (client applications)	Random: Loss and modification of information during selection, transmission, and processing. Loss of information due to improper storage of archived data. Errors during system configuration. Failures, malfunctions, and crashes of hardware and software systems. Incorrect overlaying of data layers in GIS due to improper formatting. Unauthorized destruction, modification, or copying of IP data. Blocking access to	Error detection and correction algorithms. Data hashing. Data encryption. Electronic digital signature method. Conducting periodic system configuration checks. Defining requirements for specialists who configure the systems. Logging failures, malfunctions, and crashes. Functional control of hardware and software in the information system (IS). Data backup. Automated data format verification before import. Strengthening user	Tools for implementing electronic digital signatures. Firewalls. Antivirus software. Access control and segregation systems. Checkpoints. Key and electronic locks. Alarm systems. Emergency generators. Uninterruptible power supplies (UPS). Automated attack detection system sensors. Tools for creating and storing backup copies. Change logs for configurations and algorithms.

IP data.	and process authentication mechanisms.	Hash functions, hash tables. Use of certified antivirus software. Configuring systems for protection against denial-of-service (DDoS) attacks. Regular scanning of GIS software and information for malicious components.
Targeted threats:		
Infection of databases with malicious software. Destruction or damage of hardware. Unauthorized access to information systems (IS). Disabling or malfunctioning of security systems for IS. Interception of information during different lifecycle stages. Use of malicious software or logic bombs during various stages of the information lifecycle. Violation of algorithms, configuration of hardware and software systems. Breach of integrity or authenticity of information.	Organization of internal and external secure document management. Use of backup access channels to information resources (IR). Expanding bandwidth for protection against denial-of-service attacks. Limiting access to IR/connection to the Internet. Use of certified licensed software. Control and segregation of access. Identification, authentication, and authorization. Database encryption. Data hashing. Data backup. Encryption of data processing processes. Limiting access to automated information processing systems.	Tools for implementing electronic digital signatures. Firewalls. Antivirus software. Access control and segregation systems. Checkpoints. Key and electronic locks. Alarm systems. Emergency generators. Uninterruptible power supplies (UPS). Sensors for automated attack detection procedures. Tools for creating and storing backup copies. Change logs for configurations and algorithms. Hash functions, hash tables. Regular scanning of GIS software

	Implementation of malicious software to modify spatial data. DDoS attacks disrupting GIS server operation. Disclosure of confidential information.	Conducting periodic checks of system configurations and operational modes of hardware and software. Use of certified antivirus software. Configuration of systems for protection against denial-of-service (DDoS) attacks.	and information systems for malicious components.

4. Program implementation of database encryption for ICTS: the "Kalyna" algorithm, tools of the C# programming language

The symmetric block cipher algorithm "Kalyna". For cryptographic protection of confidential data in the ICTS monitoring of carbon dioxide in the regional air ecosystem, we apply a database encryption procedure based on the symmetric block cipher algorithm "Kalyna." The symmetric block cipher algorithm "Kalyna" (DSTU 7624:2014) has the following features: it provides satisfactory, high, and very high security levels (block and key lengths of 128, 256, and 512 bits); a transparent and understandable design; an AES-like structure; four different S-boxes with optimized cryptographic properties; increased MDS matrix size; a single set of lookup tables for ECB encryption in the software implementation (improved encryption and decryption performance for different modes of operation); efficient in both software and hardware implementations, sharing common lookup tables with the "Kupina" hash function (DSTU 7564:2014). The block and key lengths in bits, as well as the corresponding number of algorithm cycles, are provided in Table 5.

Table 5
Functional properties of the "Kalyna" encryption algorithm

Block length (l)	Key length (k)	Number of cycles
128	128	10
	256	14
256	256	14
	512	18
512	512	18

The stages of the algorithm, the main ones being byte substitution in the S-boxes, row shifting, and column mixing (linear transformation using the MDS matrix), are shown in Figure 4.

Depending on the key length, "Kalyna" ensures sufficient reliability based on cryptanalysis methods: for a 128-bit block, after the 5th cycle (out of 10 or 14 cycles); for a 256-bit block, after the 6th cycle (out of 14 or 18 cycles); for a 512-bit block, after the 8th cycle (out of 18).

C# Programming Language: A modern object-oriented programming language developed by Microsoft as part of the .NET framework. C#, known for its versatility and performance, is used for creating a wide range of applications, including desktop software, web applications, mobile apps, and games. With features like garbage collection, static typing, and an extensive standard library, C# allows developers to write clean and efficient code.

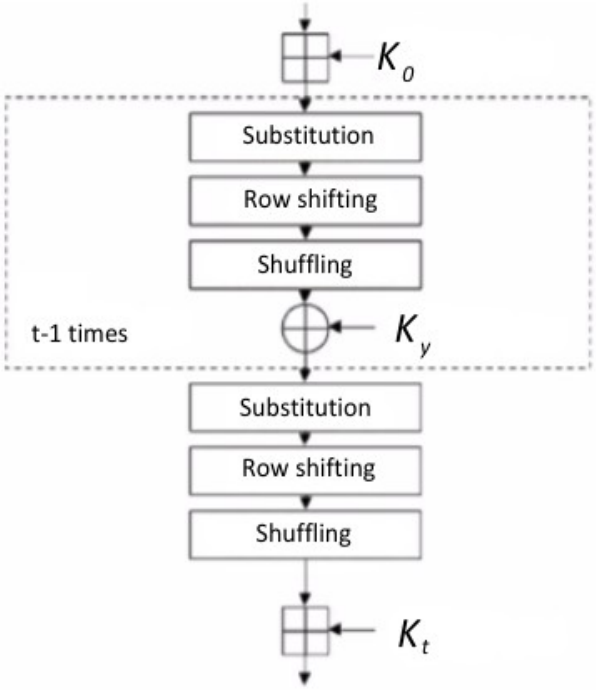

Figure 4: The Principle of Operation of the "Kalyna" Algorithm

It is especially suitable for enterprise-level applications due to its seamless integration with the .NET ecosystem and support for cross-platform development. C# is often chosen for working with databases in backend development due to its strong typing, LINQ (Language Integrated Query), and effective support for asynchronous programming. These features enable secure, efficient, and readable code for accessing databases and manipulating data. Additionally, it is used in advanced database management tools such as Entity Framework Core, providing ORM (Object-Relational Mapping) capabilities that reduce boilerplate code. In combination with ASP.Net Core, a powerful framework for creating scalable and high-performance web applications, C# and Entity Framework Core offer a robust toolkit for developing database-driven systems.

Entity Framework Core (EF Core): A modern and extensible ORM framework for .NET platform applications, EF Core allows developers to work with databases using C# objects and LINQ. It supports a wide range of databases, including SQL Server, PostgreSQL, MySQL, and SQLite, making it a versatile choice for different projects. EF Core offers features such as change tracking in databases, migrations (database updates based on code changes), and three development approaches—Code-First (Figure 5 [26]), Model-First, and Database-First.

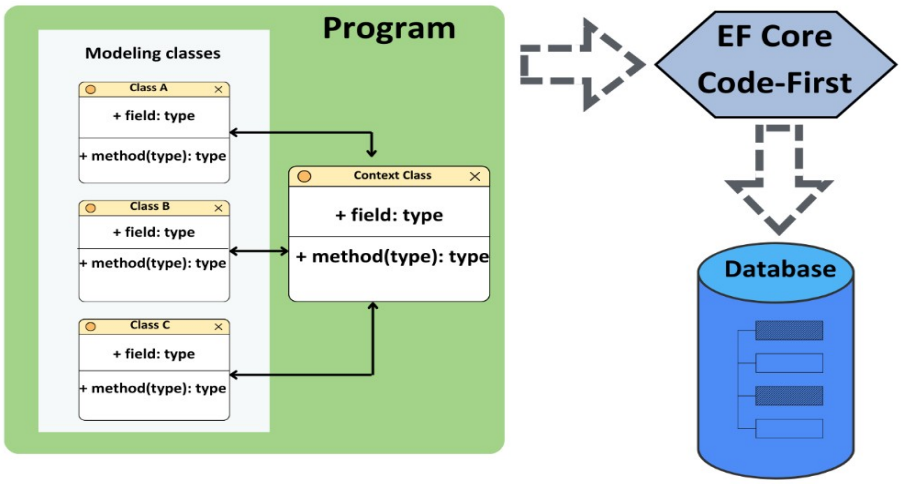

Figure 5: Code-First Approach to Database Development and Updates

These approaches allow the generation and updating of databases either from code, models, or existing databases, enabling Object-Relational Mapping, i.e., modeling a database with objects described in code and vice versa.

The software implementation of database encryption for the ICFT. Using EF Core and the Code-First approach, a database was generated in the Microsoft SQL Server DBMS. The database contains entities such as Sensor and Measurement (Figure 6), which respectively track the sensors and store information about the sampling of carbon dioxide concentration in the regional ecosystem. One sensor can conduct multiple measurements of carbon dioxide concentration, but each measurement corresponds to a specific sensor that carried it out. Therefore, the relationship between the entities in the database is one-to-many.

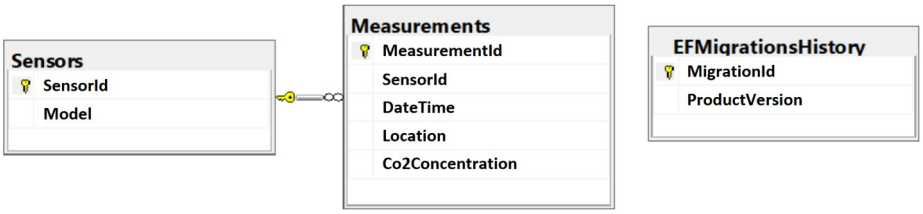

Figure 6: Database Tables

In Figure 6: Measurements stores monitoring records, and Sensors stores the installed sensors. The Measurements entity stores particularly sensitive data that require special protection, specifically the Location (location) and Co2Concentration (the measured carbon dioxide concentration) fields. Other data, such as the sensor ID or the date of the measurement, do not require encryption. This means that database encryption should be done at the field or column level, rather than at the file or table level, in order to preserve the ability to search for relevant records and work with the database without the need for decryption.

The database encryption for IKFT is carried out at the application level, as it preserves the flexibility of working with the DBMS, access to key management, and data security. The cryptographic protection software implements: encryption of selected confidential data just before storing it in the database; decryption of data during reading. The encryption implementation uses the “Kalyna-128/128” configuration, meaning both the block size and the key length are 128 bits, as the data being stored fits into a 16-byte block, and larger blocks would unnecessarily occupy database memory. However, the algorithm configuration can always be changed, for example, by applying “Kalyna-128/256” with a 256-bit key length for improved cryptographic strength.

Figure 7 illustrates the process of recording the carbon dioxide concentration measurement in the database: the sensor ID (already stored in the database), the location of the measurement, and the recorded carbon dioxide concentration value for the regional ecosystem are entered.

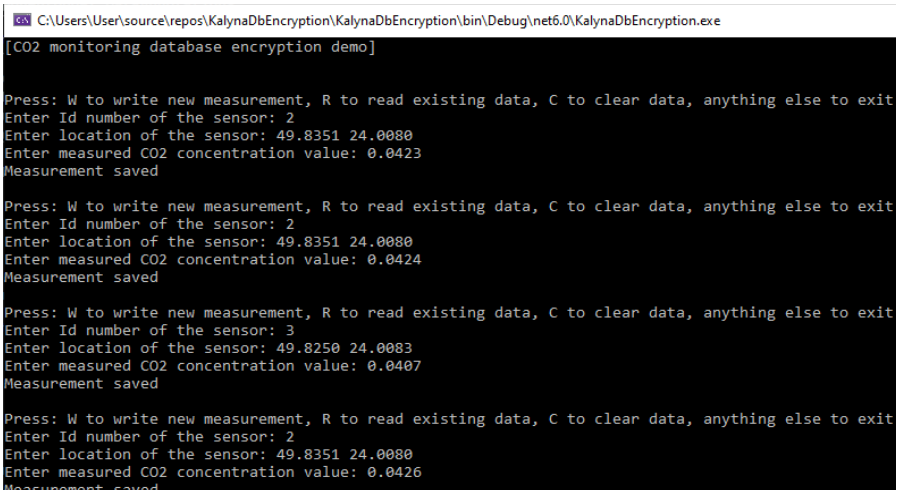

Figure 7: Recording monitoring data into the IKFT database

Figure 8 shows the data stored in the database. Since the data in the columns MeasurementId (measurement ID), SensorId (sensor ID), and DateTime (date and time of recording) are not encrypted, it is possible to work with the database and monitoring data (such as searching) without decryption. However, the data in the Location and Co2 Concentration columns is encrypted.

Results | Messages

	MeasurementId	SensorId	DateTime	Location	Co2Concentration
1	1003	2	2024-11-27 12:58:07.9205014	0xE9FD1BBE0004D29797C92488F3A43FE5	0x8673A54BCC59CA98562172C4389082AF
2	1004	2	2024-11-27 12:58:22.3892654	0xE9FD1BBE0004D29797C92488F3A43FE5	0x275143A3D065FD975A61513E7121E99C
3	1005	3	2024-11-27 12:58:35.4293168	0xA2AC50BC36AD80023CACB9BE05DB7B51	0xB7B1FA2972192232E361E4CC1AA16FD2
4	1006	2	2024-11-27 12:59:18.8764070	0xE9FD1BBE0004D29797C92488F3A43FE5	0x6FBE300E8A12F83CF41C64339DBD25A1

Figure 8: Information in the IKFT database

Figure 9 shows the data retrieved from the database using the key that was successfully used to decrypt the values in the Location and Co2Concentration columns.

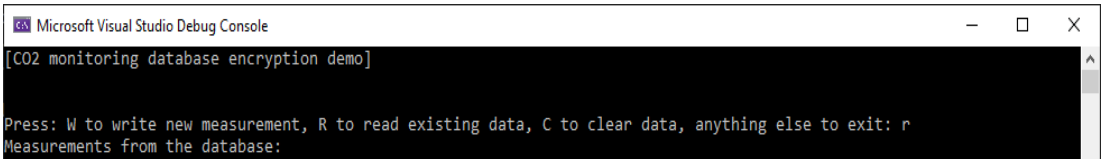

Figure 9: Monitoring data retrieved from the database and decrypted

5. Conclusion

The work presents the methodological foundations of the security of the intelligent cyber-physical technology in the air ecosystem of the region under the influence of technogenic and natural factors with (1) the architecture of the multi-level IKFT "sensors—wireless communication technologies—geographic information system"; (2) the integral model of multi-level security for IKFT; (3) integrated security systems for multi-level IKFT—physical space, communication environment, and cybernetic space according to the "object—threat—protection" concept; (4) software implementation of cryptographic protection of the IKFT cybernetic space database based on the symmetric block cipher "Kalyna" using C# programming language tools. It enables the application of the IKFT security platform as a result of the transformation of the tools, which represents the development of systemic approaches to the secure monitoring of emergency situations in the region, particularly greenhouse gas emissions for the global challenges of society.

Declaration on Generative AI

While preparing this work, the authors used the AI programs Grammarly Pro to correct text grammar and Strike Plagiarism to search for possible plagiarism. After using this tool, the authors reviewed and edited the content as needed and took full responsibility for the publication's content.

References

[1] Cybersecurity Strategy of Ukraine 2021–2025. https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeka-Eng.docx

[2] Y. Kozhedub, Y. Kramska, V. Gyrda, Analysis of Human Factor Influence on Cyber-Physical System, Inf. Technol. Secur., 8(1) (2020) 102–115.

[3] I. Opirskyy, et al., Modern Methods of Ensuring Information Protection in Cybersecurity Systems using Artificial Intelligence and Blockchain Technology, Kharkiv: Technology Center PC, 2025. doi:10.15587/978-617-8360-12-2

[4] V. Meytus, et al., Cyber-Physical Systems as a basis for Intellectualization of Smart Enterprises, Control Syst. Comput., 4(282) (2019) 14–26.

[5] Z. Ahmad, U. Islam, S. Riaz, Complexity Analysis of Industrial Scale Cyber Physical Systems, in: 2024 IEEE 7th Int. Conf. Ind. Cyber-Physical Syst. (ICPS), 2024, 1–6.
[6] S. Pogasiy, Models and Methods of Information Protection in Cyber-Physical Systems, Inf. Secur., 28(2) (2022) 67–79.
[7] O. Sholohon, Security in Cyber-Physical Systems, in: Cyber-Physical Systems Achievements and Challenges: Mater. First Sci. Semin., 2015, 132–137.
[8] M. Mandrona, et al., Generator of Pseudorandom Bit Sequence with Increased Cryptographic Immunity, Metall. Min. Ind., 6(5) (2014) 24–28.
[9] V. Bilous, et al., Cyber Evidence Software as the Digital Forensics Tools in the Investigation of Cybercrime, in: Cybersecurity Providing in Inf. and Telecom. Systems, vol. 3991 (2025) 26-37.
[10] Y. Bobalo, V. Dudykevych, H. Mykytyn, Strategic Security of the System "Object—Information Technology," Lviv: Lviv Polytech. Univ. Press, 2020.
[11] F. J. Furrer, Safe and Secure System Architectures for Cyber-Physical Systems, Inf. Spektrum, 46 (2023) 96–103. doi:10.1007/s00287-023-01533-z
[12] Y. Bobalo, V. Dudykevych, H. Mykytyn, Information Technologies for Data Collection: Concept, Methodological Approaches, Security: A Monograph, Lviv: Spolom, 2024.
[13] V. Lakhno, et al., Management of Information Protection based on the Integrated Implementation of Decision Support Systems, East.-Eur. J. Enterp. Technol., 5(9(89)) (2017) 36–41. doi:10.15587/1729-4061.2017.111081
[14] S. Mittal, et al., Cyber-Physical System Resilience, in: S. Mittal, A. Tolk (Eds.), Complexity Challenges in Cyber-Physical Systems, John Wiley & Sons, 2019, 301–337.
[15] V. Susukailo, I. Opirsky, O. Yaremko, Methodology of ISMS Establishment Against Modern Cybersecurity Threats, in: Lect. Notes Electr. Eng., Cham: Springer Int. Publ., 2021, 257–271. doi:10.1007/978-3-030-92435-5_15
[16] J. B. Nakirya, Cyber-Physical Systems: Integrating Computing with Physical Processes, Res. Output J. Eng. Sci. Res., 3(2) (2024) 49–52.
[17] Z. Yu, et al., A Survey on Cyber–Physical Systems Security, IEEE Internet Things J., 10(24) (2023) 21670–21686.
[18] S. Yevseiev, et al., Models of Socio-Cyber-Physical Systems Security: A Monograph, Kharkiv: PC Technology Center, 2023,.
[19] S. Vasylyshyn, et al., A Model of Decoy System based on Dynamic Attributes for Cybercrime Investigation, East.-Eur. J. Enterp. Technol., 1.9(121) (2023) 6–20. doi:10.15587/1729-4061.2023.273363
[20] V. Dudykevych, et al., Platform for the Security of Cyber-Physical Systems and the IoT in the Intellectualization of Society, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3654, 2024, 449–457.
[21] Regulations on the Interaction of Subjects of Monitoring, Surveillance, Laboratory Control and Forecasting of Emergencies, 2018. https://dsns.gov.ua/upload/1/2/6/3/6/2018-2-24-reglament-monatoring.odt
[22] O. Milov, et al., Development of Methodology for Modeling the Interaction of Antagonistic Agents in Cybersecurity Systems, East.-Eur. J. Enterp. Technol., 2.9(98) (2019) 56–66. doi:10.15587/1729-4061.2019.164730
[23] Carbon Dioxide Analyzer RK300-03. 2021. https://en.gassensor.com.cn/Product_files/Specifications/CM1106SL-NS%20Super%20Low%20Power%20CO2%20Sensor%20Module%20Specification.pdf
[24] Carbon Dioxide Analyzer CM1106SL-NS. 2015. https://img.yfisher.com/m6041/04e2e9a294e39c7b82321b88ab538d90.pdf
[25] F. Mukherjee, Introduction to Geographic Information Systems, United States: Rowman & Littlefield Publ., 2024.
[26] Entity Framework Core Code First: Introduction, Best Practices, Repository Pattern, Clean Architecture, 2024. https://medium.com/@codebob75/entity-framework-core-code-first-introduction-best-practices-repository-pattern-clean-22b6152bcb81