UDC 664.144:664.849
DOI: 10.15587/2706-5448.2025.325422

**Tetiana Savchenko,
Nataliia Lutska,
Lidiia Vlasenko,
Mariana Sashnova,
Andrii Zahorulko,
Sofiia Minenko,
Eldar Ibaiev,
Nataliia Tytarenko**

RISK ANALYSIS AND CYBERSECURITY ENHANCEMENT OF DIGITAL TWINS IN DAIRY PRODUCTION

The object of research is technological and technical processes that affect the effectiveness of developing a system with Digital Twins and ensuring cyber security using the example of the dairy industry.

The work is aimed at solving the problems in the sector of a comprehensive system for monitoring production processes with the possibility of early detection of deviations and potential threats. This, in turn, can lead to a decrease in product quality and an increase in cyber security risks.

During the implementation of the research, a Digital Twins of the main technological areas was developed using the example of a dairy enterprise, namely: receiving, apparatus and dietary departments. This approach provides for the collection and analysis of data on production parameters (pasteurization temperature, level in tanks, etc.), and also integrates the results of laboratory control. It was found that technological risks have the greatest impact on the effectiveness of the functioning of production processes, and security risks directly account for 35 % of the total threat structure. This is partly due to one of the main problems in the sector of insufficient data protection and possible external interference, including during cyber attacks. In addition, the analysis identified three risk groups (a total of 13 factors), which further allowed to determine their impact on the efficiency of production as a whole. This, in turn, allowed to draw a preliminary conclusion that the use of cybersecurity risk management strategies reduces the likelihood of technical failures and information threats at an industrial enterprise. The results of modeling Digital Twins of the main technological areas using the example of a dairy enterprise showed that the implementation of strategies from the security risk group increases the efficiency of the project by 4 %. The results obtained can be used to increase the level of cybersecurity and monitor production processes in the dairy industry and other agro-industrial sectors. The developed Digital Twins can be integrated into quality and safety management systems for food production, in particular, for enterprises operating in conditions of increased risks of cyber threats.

Keywords: *Digital Twins, industrial Internet of Things, monitoring, control and threat modeling, technological risks, food industry, information systems security.*

*Received: 11.01.2025
Received in revised form: 05.03.2025
Accepted: 14.03.2025
Published: 31.03.2025*

How to cite

Savchenko, T., Lutska, N., Vlasenko, L., Sashnova, M., Zahorulko, A., Minenko, S., Ibaiev, E., Tytarenko, N. (2025). Risk analysis and cybersecurity enhancement of Digital Twins in dairy production. Technology Audit and Production Reserves, 2 (2 (82)), 37–49. https://doi.org/10.15587/2706-5448.2025.325422

1. Introduction

The Industrial Internet of Things, part of the context of Industry 4.0 [1, 2], contributes to the development of the industrial sector by expanding production processes with modern devices and intelligent systems. However, they generate a significant amount of information that needs to be processed. To do this, the IIoT (Industrial Internet of Things) uses tools such as the Internet of Things (IoT), big data, cloud computing, artificial intelligence and Digital Twins (DT). The latter are a digital representation of a physical system, known as a physical twin, capable of simulating the life cycle of the system and reflecting the synchronized action of the physical twin. DT increase the monitoring of all physical objects using flexible methods, allowing access and exchange of data. Typically, in industrial applications, physical twins are technological devices, processes, including automated control systems. DT used in the operation of technological processes, as envisaged in Industry 4.0, can provide a constant check of the safety of product quality and production safety in general. In industry, Digital Twins (DT) control technological processes and automated systems, ensuring the safety of production and products in accordance with the Industry 4.0 concept. Production security includes a set of measures aimed at protecting industrial systems from cyber threats. There are three main groups of measures: physical, technological and organizational. Analysis of potential threats and security requirements allows to choose effective methods and technologies for protection. This applies to both hardware and software. This approach allows to solve the problems of detecting and predicting cyber attacks at industrial enterprises, including risk analysis and making optimal decisions on their management strategy.

Known approaches to implementing DT are not sufficiently conceptually justified, which complicates their universal application in various production engineering works, therefore, slows down the development and integration with physical twins. In particular, the following issues remain today [3]: calculation of expected benefits; DT behavior throughout its life cycle; consistency of use scenarios; levels of fidelity for each scenario; data ownership and protection; integration between virtual entities.

IIoT devices can be subject to various security threats and become the object of cyberattacks. Since they are connected to the Internet and interact with other systems, there is a risk of vulnerabilities and abuse by attackers. In particular, intrusion into the system poses a serious threat, and DDoS (Distributed Denial-of-Service) attacks on IIoT devices are aimed at overloading the network or device. At the same time, the leakage of confidential information can cause financial losses and loss of competitive advantage, and manipulation of production processes can lead to incorrect production or emergency situations. And physical threats can cause unauthorized access or incorrect operation of devices. To prevent security threats and cyberattacks on IoT and DT devices, appropriate security measures must be taken.

Technologies for protecting IIOT devices from cyberattacks are relevant due to their growing popularity and new cybersecurity threats. Attackers are constantly looking for new ways to invade systems, exploiting vulnerabilities in IIOT devices with limited resources and insufficient protection. The large number of connected IIOT devices also creates a wide surface for attackers to attack. Cyberattacks on IIOT and DT devices will have serious consequences, leading to the shutdown of production processes, damage to equipment, and leakage of confidential data. Rapid technological progress in the field of cybersecurity leads to the emergence of new types of cyberattacks and threats to production DT. This requires the establishment of necessary protection mechanisms at the DT design stage and constant monitoring and use of modern technologies and methods to detect and prevent new threats. The purpose of forming risk management strategies when designing DT for food production is to ensure the stability and security of the system. The goals include reducing the likelihood of cyber threats, effective interaction with other agents, minimizing vulnerabilities, optimizing cyber defense costs, rapid incident response and recovery, and taking into account the requirements of other affected systems. As a result, it is necessary to ensure a high level of cybersecurity and trust, taking into account limited resources and standards requirements.

According to the concept of building DT [4, 5], special attention should be paid to technical aspects: information modeling and filling, information synchronization, API (Application Programming Interface), communication, deployment, data interoperability and security, hardware and software.

Risk management of industrial projects with DT involves minimizing technological, technical and security risks over a certain period of time that lead to negative consequences and developing appropriate strategies:

$$\min_{U(R^i)} Risk(Risk(R^i), V(R^i), U(R^i), t),$$
$$Risk(R^i) = \left\langle Risk^{pr}, Risk^{tch}, Risk^{sc} \right\rangle, \qquad (1)$$

where R^i – risk factor, $i=1,...,13$; $Risk^i$ – risk value for factor i, $i=1,...,13$; $Risk$ – risk value for the technological line; $V(R^i)$ – risk consequences R^i; $Risk^{pr}$ – set of technological risk factors; $Risk^{tch}$ – set of technical risk factors; $Risk^{sc}$ – set of safety risk factors; $U(R^i)$ – risk management strategies R^i; t – time.

Determining the effectiveness of the developed system is reduced to the maximization problem:

$$\max\left(1/Risk\right) \to E_{\max}, \qquad (2)$$

where E – the efficiency of the developed system.

In the process of solving the problem, the work was divided into stages:

- identification of risk factors;
- conducting a qualitative assessment of each risk factor and determining their consequences;
- quantitative assessment of risk factors and the overall risk of the technological line;
- assessment of the impact on the efficiency of the developed system;
- identification of risk minimization strategies and their modeling for effective implementation of the system.

There are a number of methods and technologies for protecting IIoT devices that help ensure the security of infrastructure and data. Analysis of existing protection methods and IIoT security problems is reproduced in the works of domestic and foreign scientists [6–16], which contain detailed reviews, studies, methods and approaches to protecting IIoT devices. They describe various aspects of security, such as cryptography, intrusion detection, denial of service protection, access control, and others.

Currently, there is a sufficient selection of software for creating and implementing DT, which, in combination with the physical assets of the enterprise, monitor the actual state of the equipment, ensure compatibility with IIoT. Together with such tools, software for automated design or software for controlling IIoT devices is used. Comparative characteristics of known platforms for creating DT are considered in [17]. So, the software: aPriori is designed for modeling digital production, combines the functions of design for production, cooperation with suppliers and continuous development. Digital Twins for Engineering is a technology for predicting the reliability of vehicle transmission components and combines a large number of analytical scales in a single software package, and also has a computing environment. Digital Twin Organization from Interfacing contains tools for rapid application development and a management tool that makes it possible to digitize processes and increase production efficiency. AWS (Amazon Web Services) IoT provides services that cover all levels of security, including preventive measures (data access control and encryption, continuous monitoring and configuration auditing). AWS IoT also allows to create models in the cloud with subsequent deployment on devices, optimizing operations.

Siemens NX is a universal integrated solution for modeling and design of production.

A review of the literature on DT [3, 18–23] indicates a wide range of use of various modern methods, methodologies, technologies, approaches, such as classical analytical modeling methods, artificial intelligence, machine learning, ontologies, etc.

The most popular tools for IoT development were analyzed in [24]. However, it is worth noting the flexible open source visual editor Node-RED [25], which makes it possible to establish the relationship between clouds, databases, APIs, and develop software for software-hardware systems, including IoT devices. One of the advantages of Node-RED is its versatility, which makes it possible to configure individual data streams, work with a browser-based data stream editor, and individual nodes with different functionality. The lightweight runtime environment built on Node.js has the advantage of a non-blocking, event-oriented model, making it ideal for working at the Edge of the network on a variety of hardware, as well as in the cloud.

Information and communication technologies provide many opportunities for business development, but at the same time, cybersecurity threats analyzed in [26–30] are increasing, and some aspects are proving to be particularly risky. Modern cyberattacks are becoming more frequent and complex, and their wide range of impact on enterprises forces organizations to choose effective cyber risk management strategies. The approach to protecting the core resources of the enterprise based on detecting and eliminating cyber threats as they occur and improving security processes based on threat analysis conclusions is not effective enough. Since the recognition of complex cyberattacks and intrusions is a multi-stage process, risk management should be based on the cyber attack life cycle.

The iterative approach to the cyber risk assessment process is considered in the form of increasing the level of detail of each iteration or stopping the process, that is, after each stage there are decision points (continue, complete, return). Risk assessment, including their analysis, is a fundamental element of the enterprise risk management system. It provides information for decision-making on the risk management strategy, effective selection of risk reduction measures, assessment of the validity of transferring, accepting or avoiding the risk [26, 31].

The stages of risk assessment form the basis for decision-making on their priorities, appropriate measures taken, as well as the allocation of enterprise resources to manage them in order to support the optimal strategy. Cyber risk analysis involves choosing the best way to respond to cyber threats and implementing a protection plan. Monitoring and reviewing the status of cyber risks and their management are carried out throughout the risk management process to take optimal measures at the right time.

Thus, IIoT and DT use a wide range of communication platforms that combine various technologies, including physical devices (sensors, actuators, drive control devices, industrial controllers), a branched service-oriented architecture, intelligent information processing technologies, etc. When designing DT, it is necessary to lay down protection mechanisms to counter cyberattacks.

The aim of research is to develop an effective cybersecurity risk management strategy in the context of creating DT for food production, to improve cybersecurity measures using the example of the dairy industry in the context of identifying potential threats by developing countermeasure strategies and recommendations for ensuring the stability and reliability of the digital twin of food production.

2. Materials and Methods

The object of research is technological and technical processes on the example of the dairy industry, which affect the effectiveness of developing a system with Digital Twins, as well as cyber security.

Monitoring and validation of security of IIoT devices in industrial production play an important role in ensuring the protection and reliability of the network of connected devices. At the same time, the use of DT recreates a virtual model of the process, allowing to identify threats and prevent possible risks and take appropriate measures to prevent possible threats. Each IIoT asset has its own digital twin, which reflects all its characteristics, parameters and behavior, including data on the state of the device, its functionality, settings, access and other important attributes.

DT is the basis of a paradigm shift in systems engineering; therefore, cybersecurity issues must be taken into account during their design and integration in order to avoid future failures and ensure a successful transition to a new technology. As DT are integrated with existing automated process control systems and production information systems, the risks of cyberattacks increase significantly.

The functioning of production requires effective control of processes and installations to ensure high productivity and product quality. DT equipment works in tandem with a distributed production control system and is used to optimize work in real time, offering the operator optimal settings and parameters. DT includes data preprocessing, simulation models of equipment and process behavior, self-learning and decision-making modules [5, 16, 32].

DT of industrial production, in particular the food industry, includes (Fig. 1):

– equipment monitoring (DT equipment level). It allows to collect data from equipment and processes, control and analyze them to detect anomalies, optimize their operation, improve production rhythm and reduce downtime;

– monitoring of technological processes (DT process level). This allows to automate various stages of production, monitor process conditions, control temperature, concentration, pressure, etc. This helps ensure product stability and quality, reduce costs and increase productivity;

– production monitoring (DT production level). This allows to optimize production processes, including optimal resource allocation, planning production schedules and routes, and supporting production workers in decision-making. In addition, it allows to conduct virtual testing of new technologies, processes or production changes without affecting real operations, reduce risks and costs when implementing innovations, and identify bottlenecks in production.

To represent real technological objects in dynamics, DT components must be connected to physical originals to collect and organize data from the corresponding objects. For data analysis, DT must have computational and analytical models, which are currently usually implemented using artificial intelligence methods. Machine learning algorithms and data analytics can help in predicting product quality, optimizing process modes, and managing equipment.

DT development should include service interfaces for intelligent industrial applications to have access to data, as well as analytical conclusions. To ensure compliance with interoperability requirements, functional interaction and security standards should be taken into account for establishing connections between blocks. DT consists of data, computational models, and service interfaces, as depicted in Fig. 1.

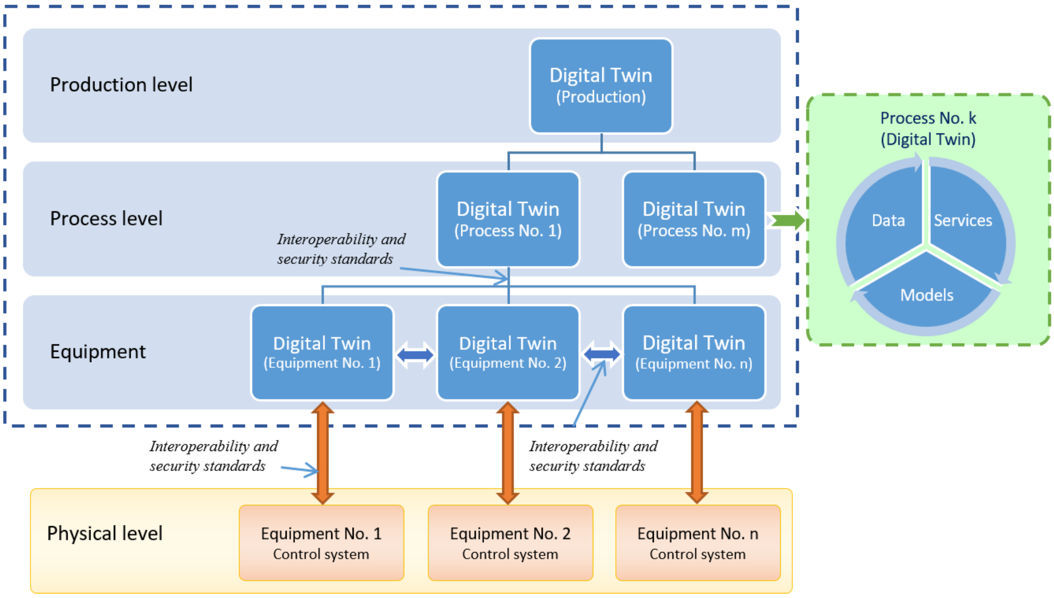

Production level
Digital Twin (Production)
Process level
Digital Twin (Process No. 1)
Digital Twin (Process No. m)
Interoperability and security standards
Equipment
Digital Twin (Equipment No. 1)
Digital Twin (Equipment No. 2)
Digital Twin (Equipment No. n)
Process No. k (Digital Twin)
Data
Services
Models
Interoperability and security standards
Interoperability and security standards
Physical level
Equipment No. 1 Control system
Equipment No. 2 Control system
Equipment No. n Control system

Fig. 1. Digital Twins of industrial production

Cyber risk assessment is a process that allows to determine the probability and consequences of cyber threats. This is an important stage of cybersecurity management, as it allows to develop effective protection measures. The work uses a comprehensive approach to assessing cyber threat risks, combining Vulnerability and Threat Analysis and an impact probability matrix. The first includes identifying potential vulnerabilities in systems and infrastructure, as well as determining possible threats that can be used to exploit them. Taking these aspects into account, potential risks are assessed and measures are taken to manage them. The second uses a matrix to assess the probability of a threat occurring and the impact of this threat on a system or organization. This allows to determine the level of cyber risk and take appropriate security measures.

Cyber risk assessment is a complex and complex task that requires the involvement of specialists from various fields. Therefore, the paper also uses the expert assessment method, which uses the experience and knowledge of experts to assess the probability and consequences of cyber threats. A modeling method is used to select the optimal cyber defense strategy.

The assessment of the probability and consequences of cyber threats is carried out in several stages:

– identification of cyber threats – potential cyber threats that can affect the system are identified;

– assessment of the probability of cyber threats – the probability that the cyber threat will be implemented is determined;

– assessment of the consequences of cyber threats – the potential impact of the cyber threat on the system is determined;

– development of strategies to increase cyber protection – protection measures are developed aimed at reducing the probability and consequences of cyber threats;

– modeling – after developing a strategy and tactical plan, implementation and implementation, modeling is carried out aimed at identifying and reducing the impact of risks on the *E* DT effectiveness.

The following hardware and software were used in the study: modern sensors for measuring technological variables, industrial controllers and their software, SCADA/HMI (Supervisory Control and Data Acquisition/Human Machine Interface – supervisory control and data collection system/human-machine interface). The type and features of the specified tools do not affect the development of Digital Twins, implemented using the tool for visual programming of data flows Node-RED, which is deployed in industrial controllers of the Edge class. Data in the Node-RED system is transmitted in JSON format (JavaScript Object Notation), which ensures ease of integration with other services and devices.

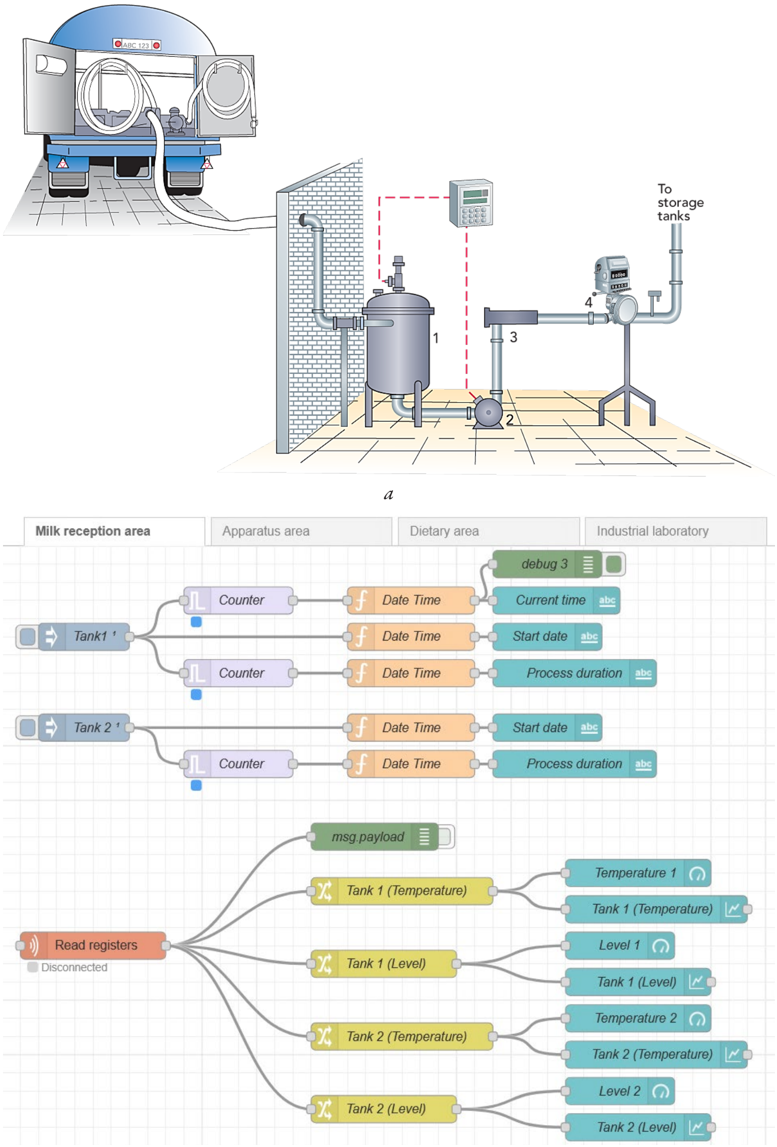
One of the limitations is that the study was based on typical production processes directly in the dairy industry. During the research, it was assumed that the sensor data is correct and up-to-date, and at the level of the digital twin there is no possibility of direct intervention in the course of technological processes through executive mechanisms. Thus, the non-destructiveness of the control level (Control Level) of the enterprise is ensured. At the same time, the main input data for modeling were typical functional schemes of dairy production, regime variables of the flow of technological processes. The proposed approach may be effective for small or medium-sized production facilities, but scaling to large enterprises may require significant changes in the hardware and software architecture and additional research.

3. Results and Discussion

The DT application for the food industry using the example of dairy production will take the form of a complex hierarchical system. Typical areas of a dairy plant are: milk reception areas, apparatus area, dietary area. Technological processes of dairy production are structurally complex, combining flows – information, material, energy. At the production level, it is necessary to take into account the loads and operating modes of each unit that makes up the production line, effectively distribute material flows and minimize risks.

Fig. 2, *a*, shows a typical diagram of the reception area of a dairy plant, where important technological parameters for controlling and managing production are the accounting of the amount of milk, the temperature and the level of milk in tanks, where milk supplied to the enterprise is temporarily stored.

To create DT tanks for temporary storage of milk at the receiving area, the Node-RED tool for visual programming of data flows was used. Using this tool, software was developed for the hardware-software system of dairy production, which includes IIoT devices for measuring temperature and level (Fig. 2, *b*).

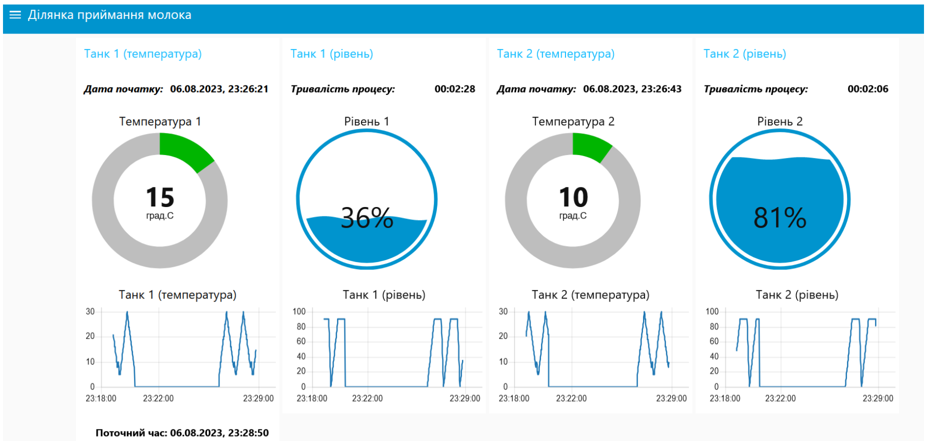


a

b

Fig. 2. Implementation of data collection of the receiving area of a dairy plant:
a – typical technological scheme of the receiving area;
b – DT of the milk receiving area

Information from sensors at the physical level is supplied to microprocessor devices (industrial controllers), SCADA/HMI. All devices are connected to an Edge-class industrial controller on which Node-RED is deployed. The results are reproduced in DT of devices, installations and technological processes (Fig. 3). A DT of the apparatus area of the dairy plant was similarly developed, a typical diagram of which is shown in Fig. 4, *a*. In particular, the DT of the pasteurization and cooling unit (Fig. 4, *b*) is presented, which is one of the main components of the apparatus area. The main parameters for control and management are the pasteurization temperature and the milk cooling temperature, which primarily affect the quality of the output product and storage times.



Дата початку: 06.08.2023, 23:26:21

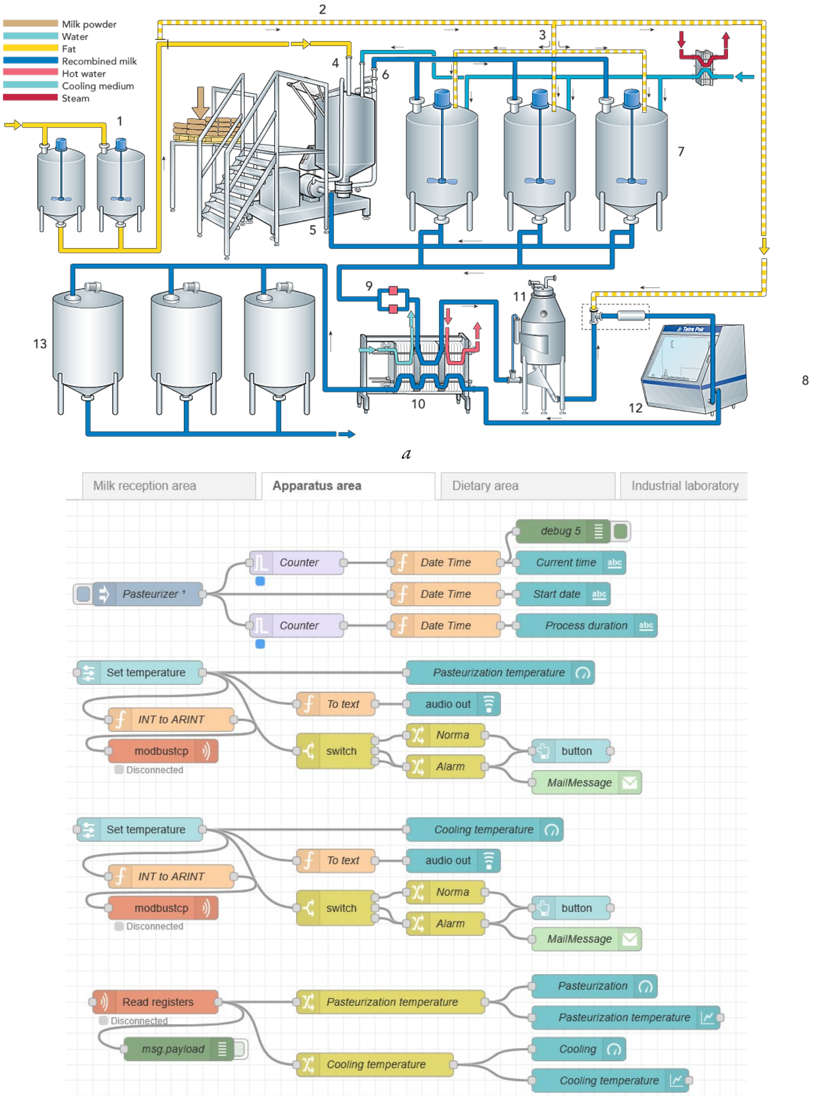
Тривалість процесу: 00:02:28

Дата початку: 06.08.2023, 23:26:43

Тривалість процесу: 00:02:06

Поточний час: 06.08.2023, 23:28:50

Fig. 3. Graphical display of temperature and milk level in tanks at the milk reception area



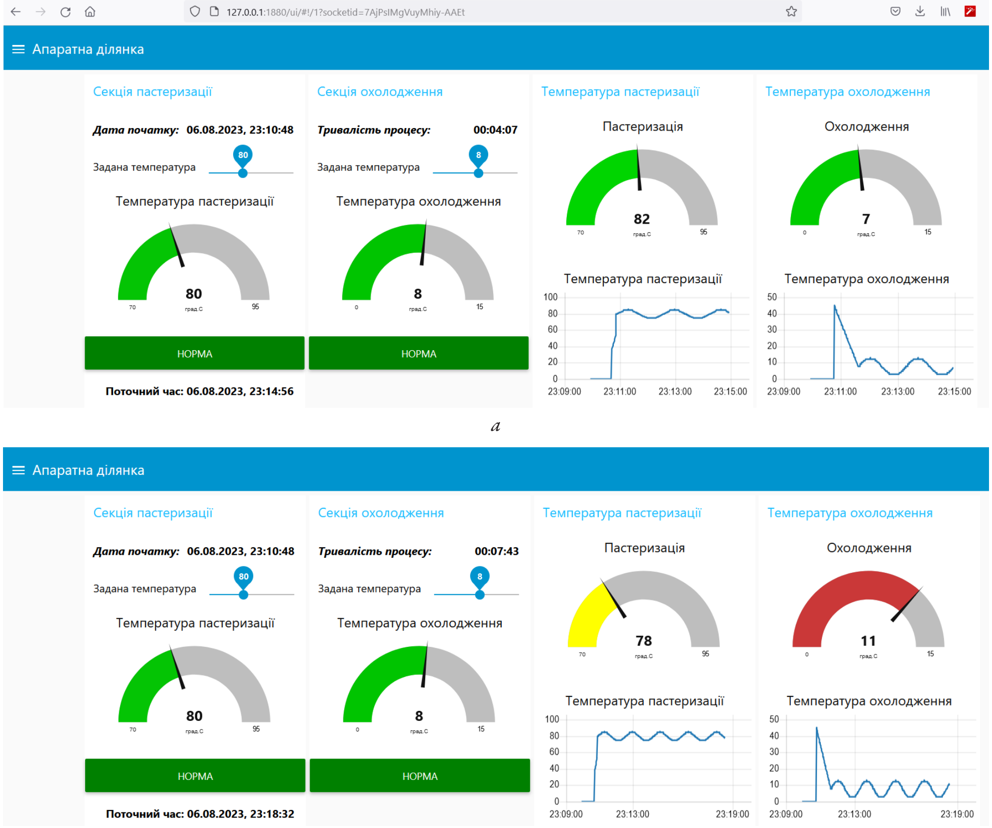
a

b

Fig. 4. Implementation of data collection of the pasteurization and cooling unit of the apparatus area of the dairy plant: *a* – typical technological scheme of the apparatus area of the dairy plant; *b* – DT of the pasteurization and cooling unit

The graphic display of the pasteurization and cooling temperature is reproduced in Fig. 5, where on the left the operator sets the set temperature value, and on the right the current temperature state of the technological process in the unit is displayed.

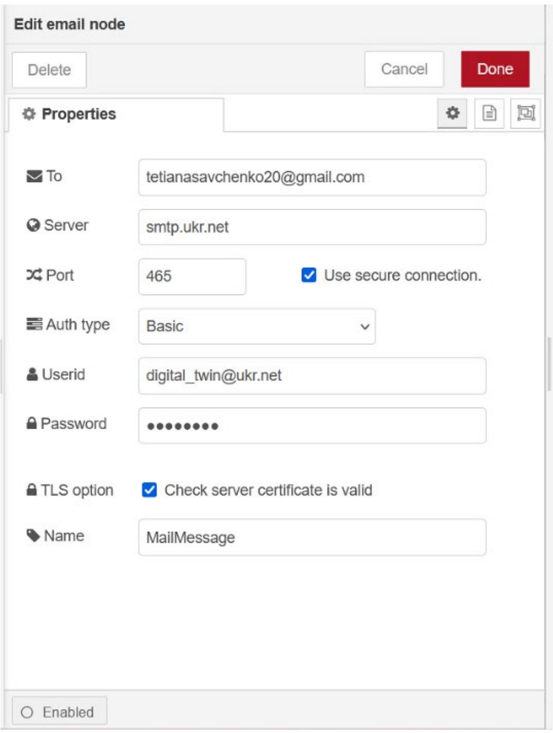
If the temperature exceeds the set value, the operator receives a message by e-mail and an alarm is triggered, which guarantees constant quality control of the production processes and their safety (Fig. 6, 7).



a

b

Fig. 5. Graphical display of pasteurization and cooling temperatures: *a* – normal operation; *b* – temperature deviation from the set value



Edit email node

Delete | Cancel | Done

⚙ Properties

To: tetianasavchenko20@gmail.com

Server: smtp.ukr.net

Port: 465 ☑ Use secure connection.

Auth type: Basic

Userid: digital_twin@ukr.net

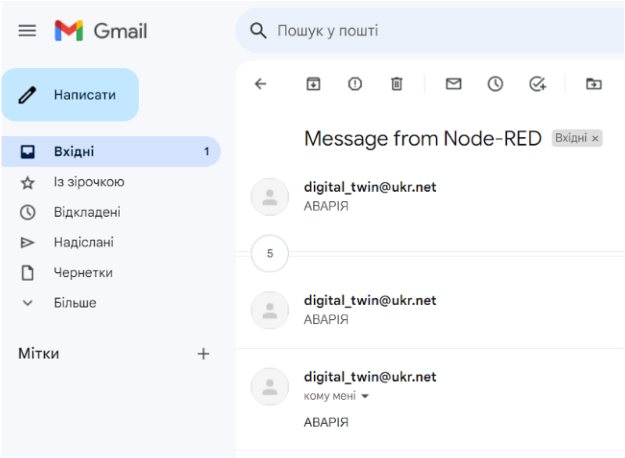
Password: ●●●●●●●●

TLS option: ☑ Check server certificate is valid

Name: MailMessage

○ Enabled

Fig. 6. Sending an emergency message



Message from Node-RED Вхідні ×

digital_twin@ukr.net
АВАРІЯ

5

digital_twin@ukr.net
АВАРІЯ

digital_twin@ukr.net
кому мені
АВАРІЯ

Fig. 7. Receiving an emergency message

Another typical area of dairy production is the dietary area, the schematic diagram of which is given in [33]. This workshop is intended for the production of various types of fermented milk products, therefore the main devices that require attention are tanks for storing raw materials and finished products, a fragment of which DT is designed and presented in Fig. 8.

The main parameters of control and management in the diet production area are the temperature and level of milk in the tanks, which is graphically displayed in Fig. 9.

The industrial laboratory in a dairy plant is an important component of the production process, as it is responsible for quality control and product safety. The main functions of the industrial laboratory include checking the quality of raw materials (e. g. milk), quality control during the production process (e. g. dairy products) and the final evaluation of the finished product before release to the market. Typical analyses performed in the industrial laboratory include determination of fat, protein, lactose, minerals, bacterial contamination and other parameters that affect the quality and safety of dairy products.

Considering the different time intervals between measurements in the industrial laboratory and in the automated plant department management systems, a separate flow was created in Node-RED for the industrial laboratory Fig. 10.

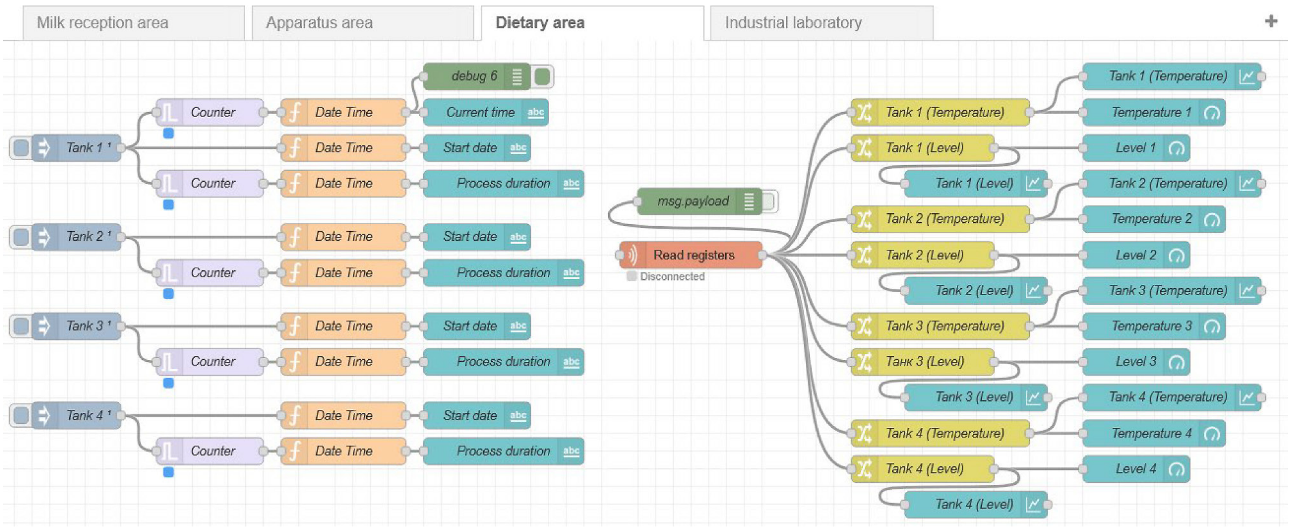
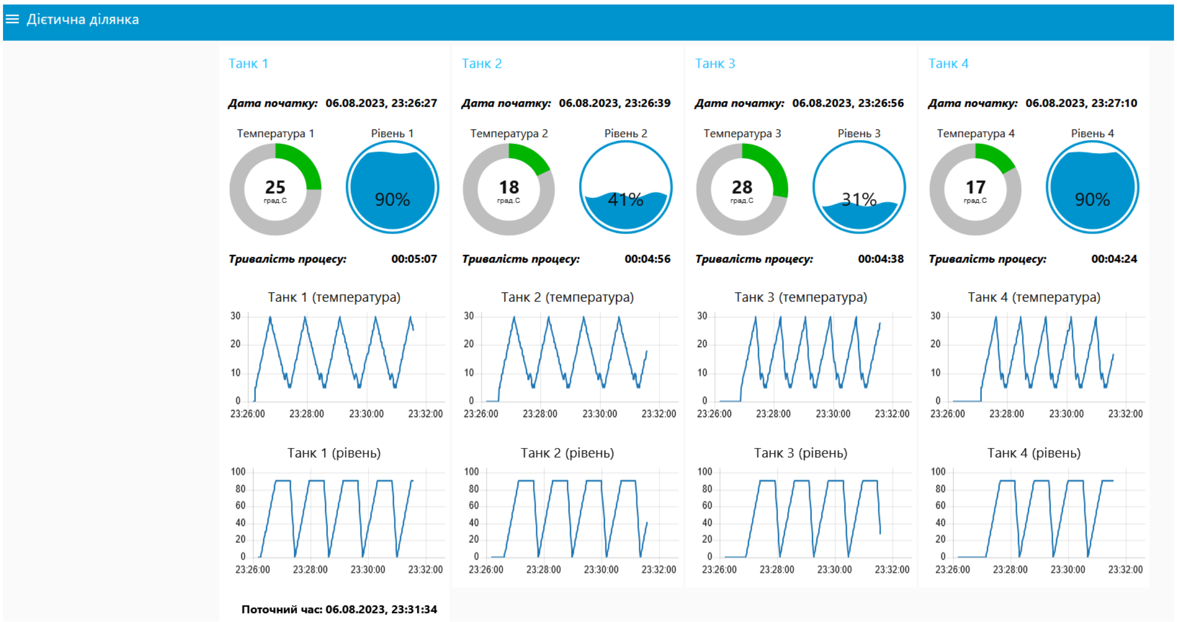


Fig. 8. Implementation of data collection for DT of the diet area



Танк 1
Дата початку: 06.08.2023, 23:26:27
Тривалість процесу: 00:05:07

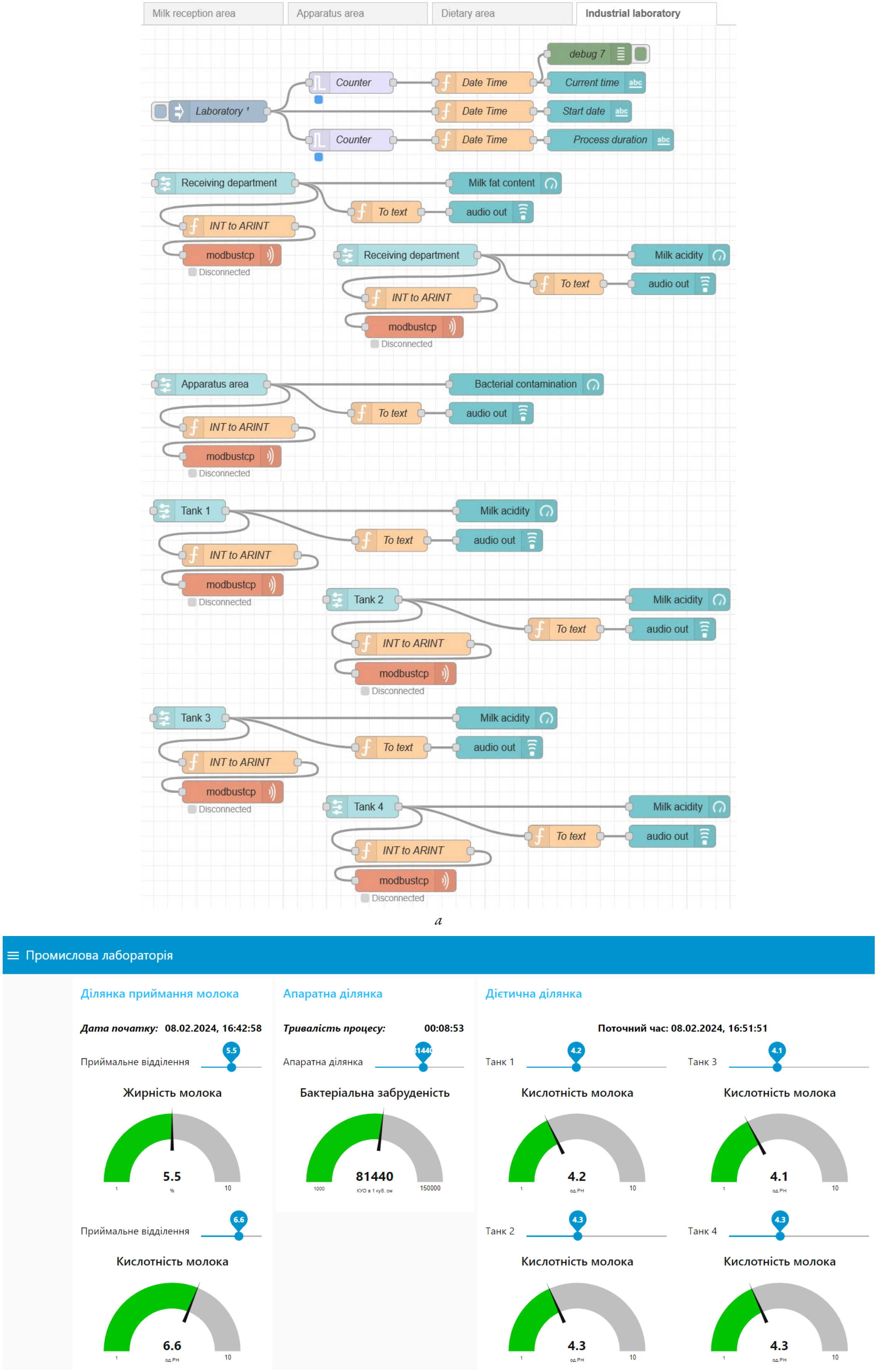
Танк 2
Дата початку: 06.08.2023, 23:26:39
Тривалість процесу: 00:04:56

Танк 3
Дата початку: 06.08.2023, 23:26:56
Тривалість процесу: 00:04:38

Танк 4
Дата початку: 06.08.2023, 23:27:10
Тривалість процесу: 00:04:24

Поточний час: 06.08.2023, 23:31:34

Fig. 9. Graphical display of temperature and level of milk in tanks in the diet area



a

≡ Промислова лабораторія

Ділянка приймання молока

Дата початку: **08.02.2024, 16:42:58**

Приймальне відділення 5.5

Жирність молока

Приймальне відділення 6.6

Кислотність молока

Апаратна ділянка

Тривалість процесу: **00:08:53**

Апаратна ділянка 81440

Бактеріальна забрудненість

Дієтична ділянка

Поточний час: 08.02.2024, 16:51:51

Танк 1 4.2

Кислотність молока

Танк 3 4.1

Кислотність молока

Танк 2 4.3

Кислотність молока

Танк 4 4.3

Кислотність молока

b

Fig. 10. Implementation of data collection in an industrial laboratory:
a – DT of an industrial laboratory; *b* – graphical display of milk quality indicators

It is assumed that the model blocks and their simulation are implemented in other Node-RED streams by involving machine learning methods, in particular, the TensorFlow.js library. Thus, using DT technology and a tool for visual programming of Node-RED data streams, a DT block was implemented for data collection for a dairy enterprise management system.

Risk assessment and recommendations for risk management may be specific to specific types of devices and systems. For example, for sensors that measure important production parameters, risks such as data loss and impact on production may be most relevant. For connected controllers or equipment that control production processes, risks associated with cyberattacks and production downtime can have a serious impact on production activities. Depending on the specific context and type of IIoT devices, recommendations may include the development and implementation of security programs, data exchange using exchange protocols, configuration of monitoring and anomaly detection systems, and physical security measures. Therefore, specific measures and recommendations for risk management should take into account the types and characteristics of IIoT devices, their use, and the specifics of the production processes they serve.

It is important that manufacturers and industrial operators thoroughly analyze their systems, identify unique risks, and implement security measures that best suit their needs and context. Table 1 below lists the main risks specific to dairy production and their consequences. It was created by analyzing the scientific and technical literature [29] on this topic and based on the experience of leading specialists (operators-technologists, automation specialists, and cybersecurity – the experts involved).

To assess technological risks, let's introduce a risk indicator that calculates the weighted probability of deviation of the average value of the main qualitative technological variable for a certain period from the permissible values of deviations of the technological regulations:

$$\Delta x^{i}_{\max} : Risk^{Ri,\, i=1\ldots3} = s^{i} p^{i}\left(\left|\Delta\bar{x}^{i}\right| > \Delta x^{i}_{\max}\right), \tag{3}$$

where x^i – the value of the main qualitative technological variable of the factor $i=1,\ldots3$; p^i – the probability of the i-th factor; $\Delta\bar{x}^i$ – the deviation of the average value of the technological variable for a certain period from the permissible values of deviations of the technological regulations; $\Delta x^i_{\max}$ – the permissible value of deviations of the technological regulations for the i-th factor; s^i – the average severity of the negative consequence of the corresponding risk factor i.

For the milk acceptance department, x^1 is one of the qualitative variables of the incoming milk (fat content, acidity, etc.), for the apparatus area x^2 is the bacterial contamination of pasteurized milk; for the dietary area x^3 is the acidity of milk (Fig. 10).

To calculate technical risks and safety risks, the formula (4) is used, which shows the weighted probability of an event A^i occurring for the corresponding factor:

$$Risk^{i=4\ldots13} = s^{i} p\left(A^{i}\right), \tag{4}$$

where A^i – the event of occurrence R^i for a certain period $i=4,\ldots,13$.

The production risk *Risk* is determined by the total risk of the flow line, taking into account the impact of the consequences on the following departments. Table 2 shows the results of calculating the risks (3), (4) of dairy production by areas and for the entire flow line. The last column determines the degree of influence of risk factors on the efficiency of the system using the Pareto rule (Table 3).

Fig. 11 presents the influence of factors on the overall efficiency of the system in percentage.

It can be concluded that the technological risk group has the greatest impact, and the technical group has the least. Security risks account for 35 % of the total, with the greatest impact being factors related to external interference and insufficient protection of various data.

DT can be vulnerable to various types of cyberattacks, including hacking, malware implementation, leakage of confidential information, and many others. Therefore, it is necessary to take measures to protect Digital Twins and ensure their integrity, confidentiality, and availability.

Table 1

Main risks and their consequences for dairy production

R^i	Risk factor content	Numerical weight of risk s^i	Risk consequences $V(R^i)$
	Technological risks $Risk^{pr}$		
R^1	Loss of quality	0.11	Product batch damage, material and reputational losses
R^2	Reduced productivity	0.12	Reduced profits, loss of sales market, reduced competitiveness
R^3	Increased losses	0.12	Increased product cost, reduced profits
	Technical risks $Risk^{tch}$		
R^4	Failure of an equipment unit	0.054	Equipment damage due to wear and tear or personnel incompetence
R^5	Environmental impact	0.046	Equipment damage due to bad weather or other natural disasters
R^6	Data loss due to equipment failure	0.091	Loss of important production data, delays in work
	Security risks $Risk^{sc}$		
	Cyber attacks		
R^7	Unauthorized access to systems	0.098	Potential loss of control over production, increased material and reputational losses
R^8	Data manipulation	0.053	Damage or loss of data, negative impact on production
	Data loss		
R^9	Production data leakage	0.027	Reputational damage, impact on competitiveness
R^{10}	Confidential data leakage	0.058	Reputational damage, possible legal consequences
	Physical risks		
R^{11}	External interference	0.057	Intentional damage to equipment due to physical impact of the offender
	Ensuring criticality		
R^{12}	Insufficient protection of important assets	0.11	Loss of control over important production processes
R^{13}	Insufficient quality of IT component provision	0.056	Negative impact on production quality, delays in work

Table 2

Results of calculating risks for dairy production

R^i	p^i of milk reception area	Risk assessment $Risk^i$ of milk reception area	p^i of apparatus area	Risk assessment $Risk^i$ of apparatus area	p^i of dietary area	Risk assessment $Risk^i$ of dietary area	Risk of flow line (production) $Risk$	Impact on E (according to the Pareto rule)
R^1	0.021	0.00231	0.009	0.00099	0.002	0.00022	0.002312	High
R^2	0.015	0.0018	0.011	0.00132	0.01	0.0012	0.001802	High
R^3	0.001	0.00012	0.004	0.00048	0.005	0.0006	0.000120	Medium
R^4	0.01	0.00054	0.028	0.001512	0.026	0.001404	0.000540	High
R^5	0.0002	0.0000092	0.0001	0.0000046	0.0001	0.0000046	0.000009	Non-significant
R^6	0.005	0.000405	0.001	0.000081	0.001	0.000081	0.000405	Medium
R^7	0.002	0.000196	0.0009	0.0000882	0.0007	0.0000686	0.000196	Medium
R^8	0.002	0.000086	0.0008	0.0000344	0.0006	0.0000258	0.000086	Low
R^9	0.001	0.000027	0.0008	0.0000216	0.0006	0.0000162	0.000027	Low
R^{10}	0.009	0.00045	0.0009	0.000045	0.001	0.00005	0.000450	Medium
R^{11}	0.012	0.001164	0.0005	0.0000485	0.005	0.000485	0.001164	High
R^{12}	0.004	0.00044	0.0013	0.000143	0.001	0.00011	0.000440	Medium
R^{13}	0.01	0.00044	0.0005	0.000022	0.0005	0.000022	0.000440	Medium

Table 3

Risk assessment

Risk value across all areas	Risk impact degree
$Risk>=0.0005$	High risk
$0.0005>Risk>=0.0001$	Medium risk
$0.0001>Risk>=0.00001$	Low risk
$Risk<0.00001$	Non-significant risk

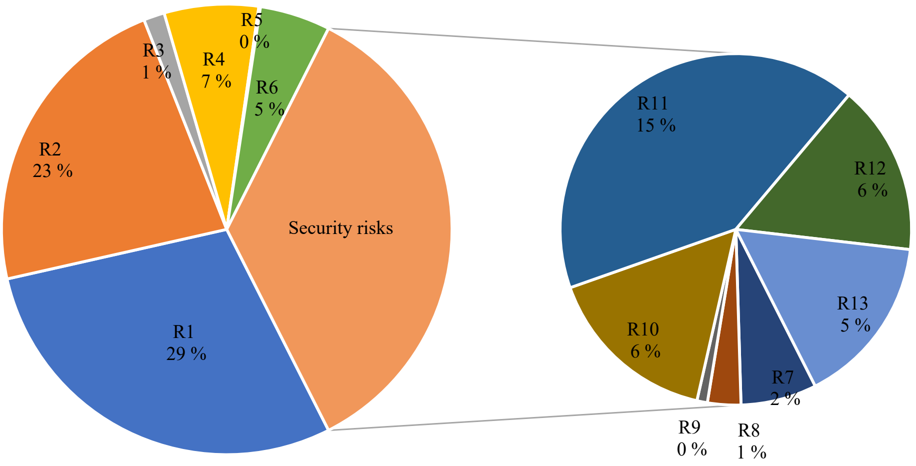


Fig. 11. Percentage distribution of risk factors

Since the Node-RED editor itself is not sufficiently secure, anyone with access to the IP address can access the editor and make changes, so it must be deployed in a securely protected network. Therefore, the developed system also needs protection, which can be implemented in the following ways:

1. Enabling HTTPS access – Node-RED can be configured to periodically update its HTTPS certificates without the need to restart it.

2. Editor and Admin API protection that supports two types of authentication: authentication based on the entered username and password, as well as authentication based on any OAuth/OpenID provider, such as Twitter or GitHub.

3. HTTP nodes and Node-RED Dashboard can be protected using basic authentication, with a single username and password granted access to routes according to the properties and settings used.

Security configurations are sensitive and should be protected from attackers. If an attacker manages to gain access to security configurations, they can use known or new vulnerabilities to launch a cyberattack or introduce a persistent threat to the system. Many cyberattacks have recently exploited security configuration vulnerabilities that can occur due to default settings or dangerous configurations that leave the system vulnerable to cyberattacks. In the case of creating a copy of the physical environment (for DT), security configurations must be transferred to the digital environment, which increases the likelihood of access to confidential information by third parties, some of whom may be hostile.

With this in mind, recommendations for risk management measures have been developed – Table 4, which include the percentage value by which each risk factor can be improved according to expert opinions.

Table 4

Recommended risk management strategies

R^i	Risk management strategies, $U(R^i)$	Δr^i, %
	Technological risks	
R^1	Compliance with technological regulations, monitoring the quality of raw materials and semi-finished products	16
R^2	Working with reliable suppliers of raw materials, materials and services. Availability of alternative energy sources	23
R^3	Ensuring resource and energy efficiency of technological processes	13
	Technical risks	
R^4	Predicting aging, periodic inspection and routine maintenance of equipment	17
R^5	Physical protection of equipment from bad weather, floods and other natural phenomena. Providing backup power and the ability to resume production	3
R^6	Regular diagnostics and maintenance of equipment. Regular data backup and recovery	8
	Security risks	
	Cyber attacks	
R^7	Establishing strong passwords and multi-level access control. Using encryption to ensure data confidentiality	9
R^8	Establishing data integrity monitoring systems. Regular data backups and recovery capabilities	5
	Data loss	
R^9	Establishing limited access to production data, transferring only clearly approved and processed production data to the cloud	5
R^{10}	Encryption of confidential data. Establishing limited access to confidential data	7
	Physical risks	
R^{11}	Physical protection of equipment from intentional damage. Providing backup power and the ability to resume production	14
	Ensuring criticality	
R^{12}	Using authentication and authorization systems to limit access, transfer only clearly approved and processed production data to the cloud. Incident detection and recovery	7
R^{13}	Regular updates and patches for software and hardware. Continuous audit and quality control of IT support	9

When introducing management strategies for risk groups, the following modeling results were obtained, which are shown in Fig. 12. As can be seen, the greatest increase in project efficiency is provided by strategies related to the group $Risk^{pr}$, the efficiency will increase by almost 4 % when introducing group strategies $Risk^{sc}$, and the least for the group $Risk^{tch}$.

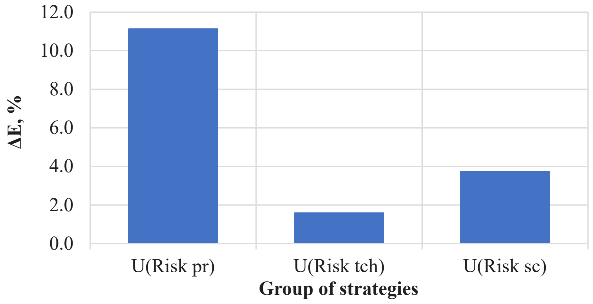


Fig. 12. Expected system performance gains

The DT accuracy compared to its physical representation is important. For example, if a digital model is subjected to a cyberattack, any predictions will be of questionable value, regardless of the relevance, interpretation, availability of data, and quality of the data obtained. However, it is important to ensure that Digital Twins are available to users who have appropriate access rights and authentication. Access control to DT and encryption of communications ensure data confidentiality and protection.

The DT use can also help detect and address cybersecurity threats. By monitoring and comparing real data with DT, anomalies, suspicious activity, and other signs of cyberattacks can be detected, allowing for timely response to threats and measures to eliminate them. In addition, it is possible to build a DT that can be used to simulate cyberattacks and determine their consequences for the system. This will allow testing of cybersecurity measures and identifying weaknesses in the system. Cyberattack simulation also helps to improve defense strategies and increase incident response readiness and reduce risks $R^7 - R^9$.

Implementing DT technology requires a comprehensive approach to cybersecurity. It is important to understand the risks associated with DT and take measures to prevent them. Ensuring the security and reliability of the system are critical factors for the successful use of DT in various industries, including the food industry. At the same time, a risk assessment will be complete only if, on the one hand, it focuses on the details, and on the other, takes into account the context of the collected data. Such DT should also include mechanisms for detecting and investigating cyber incidents that help ensure network security, protect confidential information, prevent financial losses and preserve the company's reputation. They are an important element of a comprehensive cybersecurity strategy and allow for a prompt response to threats and take the necessary measures to restore and protect the industrial production infrastructure.

The main components and functions of the DT system for responding to cyber incidents in industrial production are listed in Table 5.

Cyber incident response systems DT in industrial production can be used to implement adaptive security. The main idea of adaptive security is that the system can adapt and respond to new threats and attacks, quickly reacting to changes in cybercriminal behavior and responding to new vulnerabilities.

DT can strengthen the protection of the system by helping to detect anomalies and intrusions. They help in real-time analysis and monitoring of the system, providing early detection of potential problems, warning of possible threats and the ability to take necessary measures for protection in real time. Anomaly recognition helps to detect unusual or suspicious activity that may indicate a potential threat, while intrusion detection aims to identify actual attempts at unauthorized access or attacks on the system. This can be detected based on changes in patterns, statistical data or developed models.

Table 5

The main components and functions of the DT system for responding to cyber incidents in industrial production

Component	Function
Monitoring	DT monitors the real-time state of the cyber incident response system, including network activity, collecting information from logs, and detecting potentially suspicious activities
Anomaly analysis and detection	By comparing current data with normal system behavior, DT is able to detect anomalies and suspicious changes
Cyber incident investigation	When suspicious activity or anomaly is detected, DT can assist in investigating the incident. It collects data and information that can be useful in identifying the source of the attack and determining the cause of the vulnerability
Cyber incident response	DT of the cyber incident response system in industrial production responds to detected cyber attacks and security incidents. It provides automated procedures for recovery, isolation and elimination of threats, ensuring rapid response to incidents and minimizing their consequences
Simulation and experimentation	DT allows for simulations and experiments to determine the effectiveness of various measures for preventing and responding to cyber incidents
Security planning	Based on the collected data and analysis, DT can recommend certain security measures and improvements to the cyber incident response system
Ensuring the integrity and security of the DT itself	DT must also be protected from possible cyber attacks, as its compromise can lead to incorrect reflections of the system state and reduced response efficiency

The scientific novelty of this article lies in the development of cybersecurity risk management strategies in the context of DT development for dairy production. It is based on the identification of the main risk groups, their factors and the assessment of their impact on the overall effectiveness of the DT project. The article is of practical importance for dairy production, as it provides specific strategies and recommendations for managing cybersecurity risks when developing DT. This will allow dairy producers to effectively protect important information, ensuring the resilience of production against potential cyber threats. The implementation of the proposed strategies will help to avoid financial losses, preserve the reputation of the enterprise and ensure the continuity of dairy production in the context of digital transformation. This is a tool for improving industrial cybersecurity, which has a direct impact on the sustainability and efficiency of dairy production.

The cybersecurity risk management strategy for developing a digital twin of industrial production ensures the secure integration of digital technologies into the food industry, minimizing the threats of unauthorized access, cyberattacks, and leakage of confidential data. It contributes to the stability of production processes, the protection of recipes for multi-component semi-finished products and unique technologies, and also increases trust in digital innovations in the food sector. The implementation of multi-level mechanisms for user identification, monitoring of cyber threats, and backup of critical data allows to guarantee the uninterrupted operation of enterprises, which is especially important in the context of national food security and global geopolitical instability [34]. Prospects for further research may include a deeper study of the adaptation of cyber measures to the specific needs of food production, the impact of digital technologies on the development of the industry, and the development of innovative tools for cyber protection of industrial production.

The use of the obtained results requires adaptation to specific production conditions, in particular, taking into account the specifics of equipment and technological processes. Additionally, it is necessary to improve data processing algorithms and integrate DT with modern production management systems. An important factor is limited access to high-precision information on technological parameters due to the confidentiality of enterprise data, which may affect the accuracy of risk modeling and the effectiveness of the proposed strategies.

Martial law in Ukraine significantly complicated the research process due to limited access to production enterprises, unstable operation of logistics chains and changes in the educational process, in particular the transition to distance learning. Changes in the legislative regulation of food production safety and cyber security also had an impact, which requires additional adaptation of the proposed risk management strategies. Despite these challenges, the obtained results are relevant for increasing the resilience of dairy production in crisis conditions.

4. Conclusions

DT was obtained for the main typical sections of dairy production, which includes collecting information on the technological processes of the receiving, apparatus and dietary departments. Data on the technological parameters of production (pasteurization and cooling temperature, dairy product temperature, level in tanks, etc.). DT additionally receives data from an industrial laboratory.

It was confirmed that effective risk management is critically important for ensuring the safety and stability of production processes. Three groups of risks were identified, with a total of thirteen factors. For each factor, a numerical weight, its consequences, and the risk for each dairy production department were determined. Technological risks have the greatest impact on the overall efficiency of the system, and security risks account for 35 % of the total. Of these, factors related to insufficient protection of various data and external interference have the greatest impact.

Strategies for risk groups were proposed, which include improving technical protection measures and developing appropriate risk management procedures. Based on the modeling of risk management strategies, it was determined that the greatest increase in project efficiency is provided by strategies related to the technological risk group. The efficiency will increase by almost 4 % when introducing strategies from the security risk group. Strategies related to the technical risk group have the least impact on efficiency.

Conflict of interest

The authors declare the absence of a conflict of interest regarding this study, including financial, personal, authorship or other nature that could link the study and its results presented in this article.

Financing

The work was carried out within the framework of the state budget theme of the young scientists' project No. 1-24-25 of the State Budgetary Fund "Development of hardware and technological solutions for the production of multi-purpose polycomponent organic semi-finished products and food products in conditions of military operations and post-war reconstruction of the country".

Data availability

The manuscript has no related data.

Use of artificial intelligence

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

References

1. Hassoun, A., Ait-Kaddour, A., Abu-Mahfouz, A. M., Rathod, N. B., Bader, F., Barba, F. J. et al. (2022). The fourth industrial revolution in the food industry – Part I: Industry 4.0 technologies. *Critical Reviews in Food Science and Nutrition, 63 (23),* 6547–6563. https://doi.org/10.1080/10408398.2022.2034735

2. Pozzi, R., Rossi, T., Secchi, R. (2021). Industry 4.0 technologies: critical success factors for implementation and improvements in manufacturing companies. *Production Planning & Control, 34 (2),* 139–158. https://doi.org/10.1080/09537287.2021.1891481
3. Jones, D., Snider, C., Nassehi, A., Yon, J., Hicks, B. (2020). Characterising the Digital Twin: A systematic literature review. *CIRP Journal of Manufacturing Science and Technology, 29,* 36–52. https://doi.org/10.1016/j.cirpj.2020.02.002
4. Han, S. (2020). A review of smart manufacturing reference models based on the skeleton meta-model. *Journal of Computational Design and Engineering, 7 (3),* 323–336. https://doi.org/10.1093/jcde/qwaa027
5. Digital Twins for Industrial Applications (2020). Definition, Business Values, Design Aspects, Standards And Use Cases. *An Industrial Internet Consortium White Paper.* Available at: https://www.iiconsortium.org/pdf/IIC_Digital_Twins_Industrial_Apps_White_Paper_2020-02-18.pdf
6. Pal, S., Jadidi, Z. (2021). Analysis of Security Issues and Countermeasures for the Industrial Internet of Things. *Applied Sciences, 11 (20),* 9393. https://doi.org/10.3390/app11209393
7. Khanam, S., Ahmedy, I. B., Idna Idris, M. Y., Jaward, M. H., Bin Md Sabri, A. Q. (2020). A Survey of Security Challenges, Attacks Taxonomy and Advanced Countermeasures in the Internet of Things. *IEEE Access, 8,* 219709–219743. https://doi.org/10.1109/access.2020.3037359
8. Latif, S., Idrees, Z., Huma, Z., Ahmad, J. (2021). Blockchain technology for the industrial Internet of Things: A comprehensive survey on security challenges, architectures, applications, and future research directions. *Transactions on Emerging Telecommunications Technologies, 32 (11).* https://doi.org/10.1002/ett.4337
9. Abosata, N., Al-Rubaye, S., Inalhan, G., Emmanouilidis, C. (2021). Internet of Things for System Integrity: A Comprehensive Survey on Security, Attacks and Countermeasures for Industrial Applications. *Sensors, 21 (11),* 3654. https://doi.org/10.3390/s21113654
10. Mendez Mena, D., Papapanagiotou, I., Yang, B. (2018). Internet of things: Survey on security. *Information Security Journal: A Global Perspective, 27 (3),* 162–182. https://doi.org/10.1080/19393555.2018.1458258
11. Corallo, A., Lazoi, M., Lezzi, M., Luperto, A. (2022). Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review. *Computers in Industry, 137,* 103614. https://doi.org/10.1016/j.compind.2022.103614
12. Jhanjhi, N., Humayun, M., N. Almuayqil, S. (2021). Cyber Security and Privacy Issues in Industrial Internet of Things. *Computer Systems Science and Engineering, 37 (3),* 361–380. https://doi.org/10.32604/csse.2021.015206
13. Shepherd, C., Arfaoui, G., Gurulian, I., Lee, R. P., Markantonakis, K., Akram, R. N. et al. (2016). Secure and Trusted Execution: Past, Present, and Future – A Critical Review in the Context of the Internet of Things and Cyber-Physical Systems. *2016 IEEE Trustcom/BigDataSE/ISPA,* 168–177. https://doi.org/10.1109/trustcom.2016.0060
14. Peter, O., Pradhan, A., Mbohwa, C. (2023). Industrial internet of things (IIoT): opportunities, challenges, and requirements in manufacturing businesses in emerging economies. *Procedia Computer Science, 217,* 856–865. https://doi.org/10.1016/j.procs.2022.12.282
15. The Business Viewpoint of Securing the Industrial Internet (2016). Executive Overview. *Industrial Internet Consortium.* Available at: https://hub.iiconsortium.org/securing-industrial-internet-exec-overview
16. Caindec, K., Buchheit, M., Zarkout, B., Schrecker, S., Hirsch, F., Dungana, I. et al. (2023). Industry Internet of Things Security Framework (IISF). *An Industry IoT Framework Publication.* Available at: https://www.iiconsortium.org/wp-content/uploads/sites/2/2023/06/IISF-Version-2.pdf
17. Soori, M., Arezoo, B., Dastres, R. (2023). Digital twin for smart manufacturing, A review. *Sustainable Manufacturing and Service Economics, 2,* 100017. https://doi.org/10.1016/j.smse.2023.100017
18. Liu, X., Jiang, D., Tao, B., Xiang, F., Jiang, G., Sun, Y. et al. (2023). A systematic review of digital twin about physical entities, virtual models, twin data, and applications. *Advanced Engineering Informatics, 55,* 101876. https://doi.org/10.1016/j.aei.2023.101876
19. Attaran, M., Celik, B. G. (2023). Digital Twin: Benefits, use cases, challenges, and opportunities. *Decision Analytics Journal, 6,* 100165. https://doi.org/10.1016/j.dajour.2023.100165
20. Leng, J., Wang, D., Shen, W., Li, X., Liu, Q., Chen, X. (2021). Digital twins-based smart manufacturing system design in Industry 4.0: A review. *Journal of Manufacturing Systems, 60,* 119–137. https://doi.org/10.1016/j.jmsy.2021.05.011
21. Botín-Sanabria, D. M., Mihaita, A.-S., Peimbert-García, R. E., Ramírez-Moreno, M. A., Ramírez-Mendoza, R. A., Lozoya-Santos, J. de J. (2022). Digital Twin Technology Challenges and Applications: A Comprehensive Review. *Remote Sensing, 14 (6),* 1335. https://doi.org/10.3390/rs14061335
22. Vlasenko, L., Lutska, N., Zaiets, N., Korobiichuk, I., Hrybkov, S. (2022). Core Ontology for Describing Production Equipment According to Intelligent Production. *Applied System Innovation, 5 (5),* 98. https://doi.org/10.3390/asi5050098
23. Vlasenko, L. O., Lutska, N. M., Zaiets, N. A., Shyshak, A. V., Savchuk, O. V. (2022). Domain ontology development for condition monitoring system of industrial control equipment and devices. *Radio Electronics, Computer Science, Control, 1,* 157. https://doi.org/10.15588/1607-3274-2022-1-16
24. Lyu, Z., Fridenfalk, M. (2024). Digital twins for building industrial metaverse. Journal of Advanced Research, 66, 31–38. https://doi.org/10.1016/j.jare.2023.11.019
25. NodeREDGuidUKR. *Node-RED manual in Ukrainian.* Available at: https://pupenasan.github.io/NodeREDGuidUKR/base/
26. Hoffmann, R., Napiórkowski, J., Protasowicki, T., Stanik, J. (2020). Risk based approach in scope of cybersecurity threats and requirements. *Procedia Manufacturing, 44,* 655–662. https://doi.org/10.1016/j.promfg.2020.02.243
27. Nehrey, M., Voronenko, I., Salem, A.-B. M. (2022). Cybersecurity Assessment: World and Ukrainian Experience. *2022 12th International Conference on Advanced Computer Information Technologies (ACIT),* 335–340. https://doi.org/10.1109/acit54803.2022.9913081
28. Wu, H., Ji, P., Ma, H., Xing, L. (2023). A Comprehensive Review of Digital Twin from the Perspective of Total Process: Data, Models, Networks and Applications. *Sensors, 23 (19),* 8306. https://doi.org/10.3390/s23198306
29. Cains, M. G., Flora, L., Taber, D., King, Z., Henshel, D. S. (2021). Defining Cyber Security and Cyber Security Risk within a Multidisciplinary Context using Expert Elicitation. *Risk Analysis, 42 (8),* 1643–1669. https://doi.org/10.1111/risa.13687
30. Vlasenko, L. O., Lutska, N. M., Zaiets, N. A., Savchenko, T. V., Rudenskiy, A. A. (2024). Development of applied ontology for the analysis of digital criminal crime. *Radio Electronics, Computer Science, Control, 4,* 184. https://doi.org/10.15588/1607-3274-2023-4-17
31. Kolosok, S., Lyeonov, S., Voronenko, I., Goncharenko, O., Maksymova, J., Chumak, O. (2022). Sustainable Business Models and IT Innovation: The Case of the REMIT. *Journal of information technology management, 14,* 147–156. https://doi.org/10.22059/JITM.2022.88894
32. Voronenko, I., Klymenko, N., Nahorna, O. (2022). Challenges to Ukraine's Innovative Development in a Digital Environment. *Management and Production Engineering Review, 13 (4),* 48–58. https://doi.org/10.24425/mper.2022.142394
33. *Systema avtomatyzatsii diietdilnytsi Yahotynskoho maslozavodu* (2010). Available at: https://www.copa-data.com.ua/proekty/sistema-avtomatizatsiji-dietdilnitsi-yagotinskogo-maslozavodu
34. Zahorulko, An., Zagorulko, Al., Minenko, S., Bozhydai, I. (2024). Scientific and practical justification of innovative approaches to production of multicomponent semi-finished products for food products in the conditions of food security of the country. *Food Production: Innovative Technological Solutions.* Kharkiv: PC TECHNOLOGY CENTER, 64–91. https://doi.org/10.15587/978-617-7319-99-2.ch3

Tetiana Savchenko, *PhD, Associate Professor, Department of Informatics, National University of Kyiv-Mohyla Academy, Kyiv, Ukraine, ORCID: https://orcid.org/0000-0002-8884-5360*

Nataliia Lutska, *Doctor of Technical Sciences, Professor, Department of Automation and Computer Technologies of Control Systems named after Prof. A. P. Ladanyuk, National University of Food Technology, Kyiv, Ukraine, ORCID: https://orcid.org/0000-0001-8593-0431*

Lidiia Vlasenko, *PhD, Associate Professor, Department of Informatics, National University of Kyiv-Mohyla Academy, Kyiv, Ukraine, ORCID: https://orcid.org/0000-0002-2003-6313*

Mariana Sashnova, *PhD, Associate Professor, Department of Software Engineering and Cybersecurity, State University of Trade and Economics, Kyiv, Ukraine, ORCID: https://orcid.org/0000-0002-3501-0933*

✉***Andrii Zahorulko,*** *PhD, Associate Professor, Department of Equipment and Engineering of Processing and Food Production, State Biotechnological University, Kharkiv, Ukraine, e-mail: zagorulko.andrey.nikolaevich@gmail.com, ORCID: https://orcid.org/0000-0001-7768-6571*

Sofiia Minenko, *PhD, Senior Lecturer, Department of Management, Business and Administration, State Biotechnological University, Kharkiv, Ukraine, ORCID: https://orcid.org/0000-0003-3033-1911*

Eldar Ibaiev, *PhD Student, Department of Equipment and Engineering of Processing and Food Production, State Biotechnological University, Kharkiv, Ukraine, ORCID: https://orcid.org/0000-0003-3090-3553*

Nataliia Tytarenko, *Department of Equipment and Engineering of Processing and Food Production, State Biotechnological University, Kharkiv, Ukraine, ORCID: https://orcid.org/0000-0002-9745-883X*

✉*Corresponding author*