Information & Security

Published since 1998

V.V. Nekhai, M. Dorosh & V.A. Nekhai
vol. 46, no. 2 (2020): 168-181
https://doi.org/10.11610/isij.4612

ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

Using the Cyber Situational Awareness Concept for Protection of Agricultural Enterprise Management Information Systems

Valentyn V. Nekhai* (✉), *Mariia Dorosh*, *Valentyn A. Nekhai

Chernihiv National University of Technology, Chernihiv, Ukraine
https://www.stu.cn.ua

ABSTRACT:

There are similarities in information management between military and agricultural systems, e.g. distribution, impact of the environment, mobile agents, and the human factor are functioning in 2- and 3-dimensional space. This allows spin-offs in the implementation of the concept of Cyber Situational Awareness (CSA), which is studied intensively in the defence field, but so far has not been applied with the aim to protect agricultural enterprise management systems.

The purpose of this study is to substantiate the directions for the implementation of the CSA concept for the protection of corporate networks of agricultural enterprises, with the hypothesis that this will allow effective protection. The methodological basis is formed by the current provisions of the CSA concept, system analysis and synthesis.

Results. The stability of communication channels and security is largely determined by the reliability of data transmission in the network, which is ensured by the design of the appropriate network structure. This in turn will provide opportunities to implement the first level of the CSA concept in IT to protect agricultural management systems.

ARTICLE INFO:

RECEIVED: 31 MAY 2020
REVISED: 04 SEP 2020
ONLINE: 18 SEP 2020

KEYWORDS:

Cyber Situational Awareness, network protection, information system, control system

✉ Corresponding Author: Tel.: +380937752052; E-mail: kilavv@live.com

Introduction

Agricultural sector is one of the most successful in the economy of Ukraine, that is why its investment attractiveness is quite understandable. Furthermore, pending the Act of land privatization, increases the risks of misappropriation of efficient enterprises of the given industry.

Through considerable use of automation management systems by agricultural enterprises which are corporate networks, storing a great amount of information, there appear new possibilities of getting data and preventing of organization activity.

Automatization of technological processes management in agriculture has its own distinctions conditioned not only by technological and technical conditions of agriculture production, but a multitude of technico-technological decisions that often impede to typify the engineering solutions concerning technological processes management automatization. They are characterized by a discrete mode of equipment operation, a necessity of frequent change of operating mode influenced by external factors, a need of mobile implements utilization, operators who control them and cultivate the large land area Automation management of a technological process in agriculture production depends not only on external nature factors but on human ones, that is determined by operators skill, their social standard etc.

The efficiency of management system depends, above all, on the quality of information backing. In the system of agricultural enterprises management, there exists a great data file received from technical devices and actual data from specialists.

The specificity of industry towards corporate networks defence concerns, to our mind:

The specifics of the industry in the direction of security of corporate networks of agricultural enterprises in our opinion are:

- Low level of services
- Insufficient monitoring of information security systems
- Low level of awareness of users of agriculture automation system of management in the sphere of information security
- Underestimation of the part of defence system by enterprise management.

All these circumstances result in appearance of threats of meddling into corporate networks as on the part of external malefactors and internal ones that may result in divergence from planned activity in agriculture production foreseen by planning system, process charts and provision of special type of automation production management sub- systems - automation systems of operating management.

Thus, under rigorous competition and rising level of cyber criminality, agriculture automation systems require the development of special methods and models of their respective defence taking into account industry characteristic properties.

Methods

Modern conceptual theses of Cyber Situational Awareness are the theoretical and methodological basis of the research.

By means of the methodology of system analysis and synthesis has been carried out approaches research aiming to formation of principle directions of using CSA to defend the automation system agricultural enterprises management.

Related works

As the authors note, Franke, Ulrik, and Joel Brynielsson.[1] Cyber situational awareness attracts a great attention. It is clearly reflected in national cyber strategies of various countries, and there are a lot of researches devoted to the matter. The most of them deal with the cyber security. But up to now, there have been no attempts of using the concept to control enterprises activity, especially in agriculture.

According to a study consisting of 102 scientific papers by Franke and Brynielsson,[1] the theoretical study of cyber situational awareness focuses more on data analysis, data merging and responding to cyber threats by technical means.

But Hausken et al.[2] note that the process of attack and defence largely depends on the structure of the system, defence measures, tactics and circumstances of the attack. The structure of the system defines the goal, which can be one element, several elements, interdependent systems and networks.

Having researched the areas of use of the Cyber Situation Awareness Concept, it is possible to state its application at the state level of information resources protection and directions of research in a purely mathematical direction concerning the philosophy of the concept and its use in other areas is practically not traced in scientific publications. This assumption is confirmed by the successive publications (Cyber situational awareness - A systematic review of the literature) by Ulrik Franke and Joel Brainilsson. His research interests include website mining, uncertainty management, information merging, probabilistic expert systems, decision support, command and control, operations research, game theory, privacy protection, data mining and computer security education), but today more and more the used of this concept in other areas.

For example, the Cooke et al. [3] consider Cyber analysis as a complex task that requires the coordination of a large sociotechnical system of human analysts working together with technology. They define Teamwork in the form of communication and information coordination is at the heart of team-level situation awareness, and form suggestions for improving teamwork in the cyber domain are offered.

Recently, there have been publications on agriculture.

So, the authors [4] note that smart devices are widely used by a range of people from farmers to entrepreneurs. These technologies are used in a variety of ways, from finding real-time status of crops and soil moisture content to deploying drones to assist with tasks such as applying pesticide spray. However, the use of IoT and smart communication technologies introduce a huge exposure to cybersecurity threats and vulnerabilities in smart farming environments. Such cyber-attacks have the potential to disrupt the economies of countries that are widely dependent on agriculture. The paper outlines a multi layered architecture relevant to the precision agriculture domain and discusses the security and privacy issues in this dynamic and distributed cyber physical environment. Furthermore, the paper elaborates on potential cyber-attack scenarios and highlights open research challenges and future directions.

A thorough study in this area is also a NCC Group publication on Cyber Security in UK Agriculture, highlighting that securing farms poses some unique challenges, including low awareness of cyber security in the farming community. Relying on farmers to adopt generic guidance on how businesses can protect themselves is likely to prove ineffective by itself.

As a result of the analysis, the issue of designing the structure of the corporate network based on the actual state of network coverage (4-G technology remains imperfect in most regional areas) and the availability of own resources of agricultural enterprises remains insufficiently defined.

The main purpose of this applied study is to explore the possibilities and substantiate the directions of implementation of this concept for the protection of corporate networks of agricultural enterprises of Ukraine.

Awareness of the Situation

If you look closely at military systems and agricultural systems, you can find many eastern features: distribution, very high environmental impact, mobile agents, the human factor, functioning in 2-dimensional or 3-dimensional space, and so on.

The growing and evolutionary nature of cyberattacks and threats in computer information systems has led to the need to find new approaches and methods of information protection. In 1995, an article was published by Mica Endsley, Head of the US Air Force Research Unit,[5] which gave a general definition of the concept of awareness of the situation, which is described as follows: perception of the elements of the environment in the amount of time and space, understanding their meaning and projecting their state for the future. The application of this concept can cause much controversy in the field of economic security management, but one of the main aspects of situational awareness is its dynamism, i.e. the ability to respond in a timely manner to new and changing threat models, which is in direct conflict with the classical economic security paradigm.

Perception, understanding, projection of the current situation and assessment of possible consequences and appropriate response cannot happen without people – analysts, administrators, operators, etc.

M. Endsley's model presents three levels of situation awareness, perception, understanding and projection, later, taking into account the human factor and the use of the concept of situational awareness, McGuinness and Foy [6] and Onwubiko and Owens [7] identified the fourth level – permission.

In the new paradigm of operational management, the management system and its protection can be presented as a situational awareness of the internal state and the environment and an adequate response to the level of the identified threat. Adapting the concept of CSA to build a system of operational management of agricultural enterprises can offer the following approach (visualised on figures 1 and 2).

Level 1. Perception of the situation.

At this level, the collection of information about the state of the control object through the actual collection of information (for agricultural enterprises is an actual survey of fields, soil analysis, inventory of agricultural machinery, the availability of fuels, seeds, fertilizers, pesticides plants, etc.) and technical devices (GPS sensors, controllers, data obtained from aircraft, remote sensing satellite data, etc.). The dispatching service determines the comparability of information obtained from different sources and determines its reliability. Deviations between the actual and planned controlled parameters and possible vulnerable areas in the enterprise and management system are identified. At the level of perception, information about the state of the object of control and possible changes, both internal and external, allows you to expand the classification of states of the object of control into meaningful ideas, which are the basis for the following levels: understanding, projection and resolution.

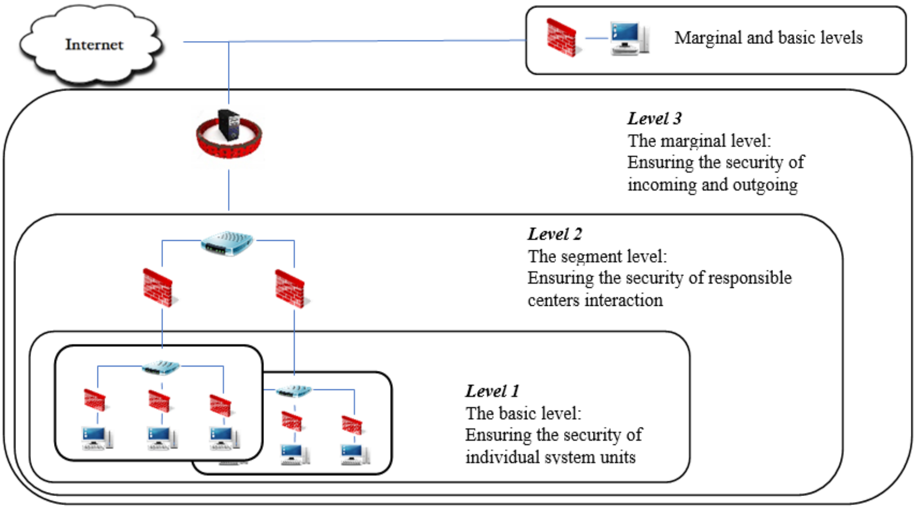

Figure 1: The model of operational understanding of the situation by Endsley.

Level 2. Understanding the situation.

At this level, the specialists of the dispatching service use a number of tools, methods for aggregation, analysis, generalization and comparison of individual parts of information and analytical support in order to determine the risks and the probability of their occurrence.

Thus, understanding is a scenario of the current situation which is realized by determining the significance of the obtained evidence of risks and threats to be monitored.

Level 3. Projection.

At this level, possible scenarios are predicted. The accuracy of the forecast for the future can be improved through the use of powerful monitoring systems and technologies that can detect and predict the patterns of future events, such as the use of early warning, which will improve planning and use of preventive control to prevent adverse situations.

Level 4. Permission.

At this level, senior management decides on the implementation of the relevant scenario and gives permission for its implementation.

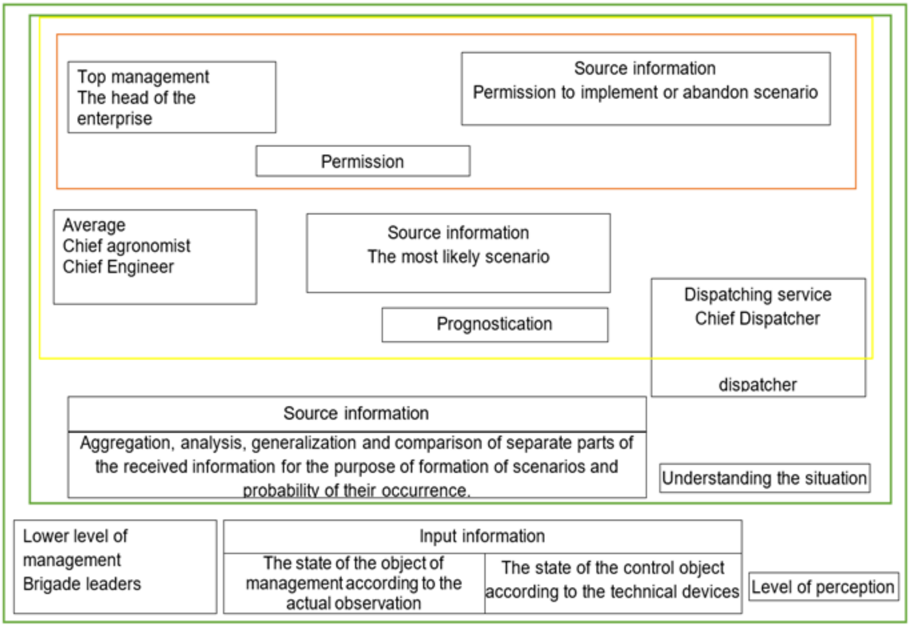
Top management
The head of the enterprise
Source information
Permission to implement or abandon scenario
Permission
Average
Chief agronomist
Chief Engineer
Source information
The most likely scenario
Prognostication
Dispatching service
Chief Dispatcher
dispatcher
Source information
Aggregation, analysis, generalization and comparison of separate parts of the received information for the purpose of formation of scenarios and probability of their occurrence.
Understanding the situation
Lower level of management
Brigade leaders
Input information
The state of the object of management according to the actual observation
The state of the control object according to the technical devices
Level of perception

Figure 2: Conceptual model of application of the CSA concept in operational management of agricultural enterprises.

Sensors and controllers

In the new paradigm of operational management, the management system and its protection can be presented as a situational awareness of the internal state and the environment and an adequate response to the level of the identified threat.

According to experts, significant progress in the use of precision farming devices is expected in the coming years. Farmers will be able to better control sowing, will be able to set economic thresholds for tactical and strategic decisions, will manage the enterprise to a new, more dynamic level, when workers will not be able to make a mistake except when it is done intentionally. It is also expected to increase the capabilities of sensors, namely users will receive more data, improve accuracy, reduce weight and cost, which will allow their use by small agricultural enterprises.

The functionality of modern sensors is increasing almost every month. We are talking about both accuracy and the ability to capture several parameters simultaneously.

Wireless sensors are used to collect data on groundwater availability, soil compaction, soil fertility, leaf temperature, leaf area index, plant water status, local climatic data, insect / weed infestations, and more.

An example is the Smart firmer sensors that Precision Planting puts on drills. They can measure soil moisture, organic matter content and the amount of crop residues in real time, with which you can get basic indicators and change the settings of tools (drills, fertilizer spreaders, sprayers) online.

High-precision fuel level sensors are designed to measure the level of fuel in the tanks of vehicles and in tanks (eg tanks). The accuracy, reliability and functionality of these devices allows them to be used as part of control systems and satellite GPS monitoring.

The sensors installed on the working units inform about the working time, the amount of work performed, the amount of fuel in the tank, speed, weighing results, which in real time allows you to get information about the type of field work, what equipment is involved, its exact location . Monitor workers - in case of fuel spills, grain spills, speeding violations, unauthorized work, downtime, deviations from the route, etc. Hummingbird platform uses unique algorithms for machine learning and artificial intelligence to process images of satellites remote sensors, UAVs small aircraft.

Taranis management decision support system includes several technologies. The first is weather forecasting technology. With an accuracy of 90% in the next 48 hours in a particular field, the user will be able to see: the amount and probability of precipitation, temperature and humidity, wind speed and leaf moisture. It is possible to see the hourly, daily and current weather forecast, as well as weather factors in the past days for each field.

Information flows and communication channels

Taking into account the specifics of agricultural enterprises and information needs of operational management of agricultural enterprises, we have identified the following objects of management, communication channels, information flows (Fig. 3).

The possibility of external and internal interference in the information system of the enterprise can affect the distortion of such parameters of information as confidentiality, integrity, accessibility, reliability, etc. This, in turn, can lead to negative consequences in the enterprise:

- Failures in the operation of technological and management process management systems
- Disclosure of information constituting commercial and other types of secrets
- Violation of the reliability of financial statements
- Unauthorized access to the enterprise database
- Distortion of public information.

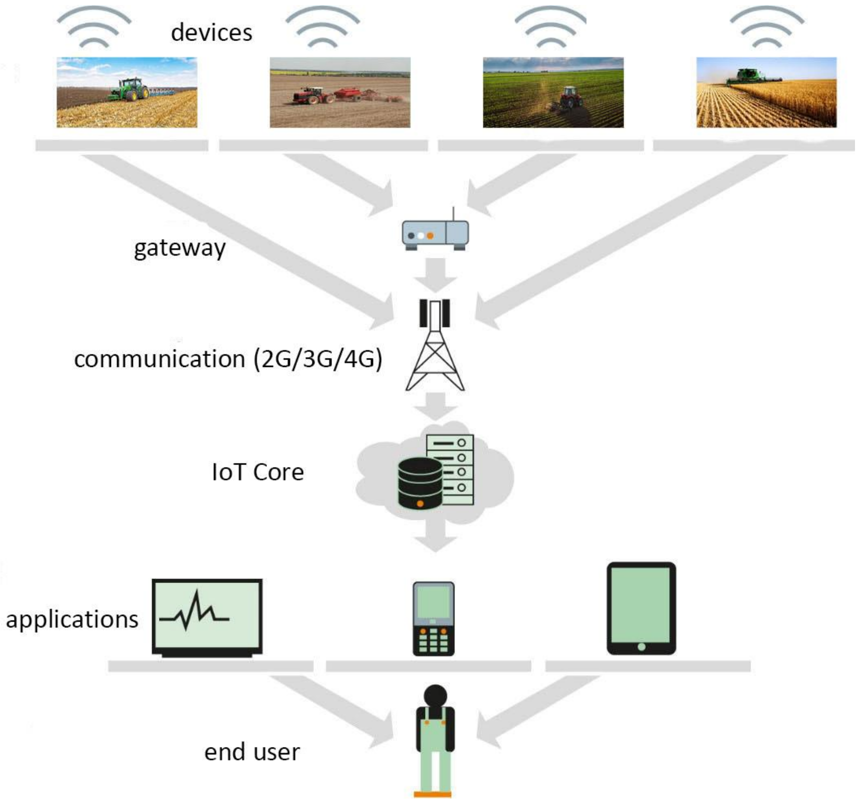

Figure 3: Communication channels for receiving data.

The stability of communication channels and security is largely determined by the reliability of data flows in the network. Physical layer corruption that often occurs on computer networks results in changes that require routing tables to be updated. In comparison, the topology (structure) of the network has a more significant impact on the stability of software than the support of physical layer technologies (ATM, Frame Relay or others).

The data transmission network is an integral part of the infrastructure of any automated system of a modern agricultural enterprise. Depending on the size of the enterprise (small, medium or large business) or field of activity, computer networks may differ from each other, for example, in architecture and scale, in the level of controllability and reliability, in the number of integrated functions. Each geographically isolated part of the enterprise (separate office, complex of buildings, agricultural lands, etc.) has its own local network, the main of which (in most cases) is the leading local data network (LAN).

Local area networks solve the following tasks:

- Data exchange between stationary or portable workstations (computers) of employees located in one office or building
- Access to corporate servers, applications or applications located in a geographically isolated part of the enterprise ("local servers"). This task is one of the most common when designing the IT infrastructure of the enterprise
- Organization of a distributed infrastructure of network services, which does not go beyond the geographically isolated part of the enterprise. A distinctive feature of this class of tasks is the requirement to provide power to end devices through a signaling interface through which they connect to the network (Power-over-Ethernet technology)
- Merge multiple local servers into a single computing cluster. Clustering is the most common method of creating a reliable and fault-tolerant corporate service (regardless of its type or purpose).

Wireless data networks.

Fast and secure access to servers of applications / applications / resources of the Internet: organization of access to the data transmission network for mobile devices; ensuring high speed and quality of service; protection of data from interception or modification, as well as protection of mobile devices from hacking attempts.

Secure wireless communication for specialized technological systems: organization of a service for communication of mobile devices with control servers and databases to ensure the automation of technological processes.

Connect leading network segments over wireless connections. Construction of wireless communication channels for data transmission in cases where there are no alternative wired connection methods. The solution is also used to provide communication on moving objects (agricultural machinery).

Integration with geographic information systems.

Unloading the network of GSM operators in places of large crowds of client devices by automatically changing the method of data transmission using Wi-Fi technology.

Distributed corporate networks (wan) In any case, there will always be a need to share shared corporate resources. Therefore, separate remote physical LANs need to be combined into one logical distributed corporate network (WAN). Distributed corporate data networks solve the following tasks:

Secure integration of geographically distributed local network segments into a single corporate data network. If you use, for example, a public unsecured Internet to communicate between remote network segments, there is a risk that your privacy or data integrity will be compromised. Therefore, the protection of corporate information transmitted by any non-corporate communication channels is a mandatory requirement for a WAN network. The most common method of such protection is the creation of a secure "virtual private network" (VPN) with mandatory authentication of network nodes and data encryption.

Introduction of a centralized remote connection hub (VPN server). This is a modified case of the main task (creating a WAN-network). The difference is that remote “networks” consist of a single workstation. Such workstations can belong to both mobile employees of the enterprise and partners of the company (customers, suppliers, remote technical support, etc.).

Ensuring priority transmission of sensitive data and general control over the use of existing communication channels (support for QoS mechanisms). Typically, external communication channels have significantly less bandwidth than internal channels within a local area network. Between different corporate services that use a distributed network, there is often competition for its resources. Such competition leads to the loss of some data of one or, in the worst case, all services.

Optimization and compression of data for the most efficient use of existing communication channels. In some cases, QoS mechanisms alone cannot guarantee the high quality of corporate services data transmission over a distributed network. An example is a situation in which the transmission of priority type data requires higher bandwidth channels than existing ones. In this case, you need to either increase the bandwidth of existing WAN channels, or use a set of data optimization methods (eg, deduplication, compression, caching, etc.). Software-configured networks (SDN).

The most pronounced and common tasks of the new generation of networks include:

- Support for mobile users (BYOD)
- Growth of traffic volumes and change of its structure in the direction of unified communications and video
- Work with cloud services and data virtualization
- BIG DATA processing.

If you look at these tasks from the point of view of the tasks of the principles of network operation - they all mean the need to provide flexible and centralized management of traffic transmission and processing. And this is exactly the possibility given today by SDN - software-configured (or conditional) network.

SDN is a data network in which the level of network management is separated from data devices and implemented in software, one of the forms of virtualization of computing resources.

The principle of construction of such networks means that the router or switch serves only a data stream (physical data transfer), to become simpler accordingly cheaper. And all the intelligent component (CLI, embedded web server or API and control protocols, as well as algorithms and functionality for automatic response to traffic changes) is transferred to the SDN controller.

This principle of network construction is implied as the classic direct commands of the system administrator to the controller. And launch network management applications on the SDN controller. Such applications are essentially a network optimization interface for a specific business application and its main role is to change the network in real time for the current tasks and needs of the serviced program. For example, this could be changing the QoS network between two telephone subscribers to transmit an HD video call in real time without delay or creating a VPN tunnel between the two subscribers.

The key advantages of such a network architecture are:

- Increase the efficiency and comfort of users with applications
- Simplification of management and reduction of time of deployment of networks at scaling
- Centralized analytics system that allows you to adjust the network in real time for current tasks
- The ability to reduce the deployment time of security tools on many objects due to unified policies and settings of their work. Network infrastructure data centre.

The data centre is a specialized facility designed to accommodate the subsystems of calculation and data storage. The most important goal of creating a data centre is to consolidate a variety of resources (power supply, cooling, cabinet space, fire extinguishing, communication channels, administrative resources, etc.), which reduces the total cost of infrastructure ownership.

There are commercial and corporate data centres according to the method of ownership. The latter can be placed not in a separate building, but in a separate specialized room directly on the territory of the enterprise. In addition to the building itself (or a separate room), engineering and telecommunications infrastructure are mandatory and integral components of the data centre. The basis of the telecommunications infrastructure is a wired data network, or network infrastructure data centre (DC LAN).

Tasks to be solved for data centres using network infrastructure.

Creating a reliable high-bandwidth transport network with ultra-low transmission delays. Reliability and high bandwidth are the most important characteristics of the network, without which it is impossible to guarantee the continuous operation and high performance of services hosted in the data centre. In addition, there are classes of tasks, such as stock trading, for which the critical parameter is the delay in data transmission (satisfactory delay should be less than 1 microsecond).

Consolidate multiple servers into a single computing cluster. Clustering is the most common method of creating a reliable and fault-tolerant corporate service (regardless of its type or purpose). The size of server clusters located in the data centre can reach dozens, or even hundreds, of physical servers. Therefore, the relevant network infrastructure should scale freely without creating bottlenecks (congested internal communication channels).

Consolidate resources and create a converged data network that combines the functions of a traditional data network (LAN) and a storage network (SAN). To reduce the total cost of ownership, as well as to ensure maximum flexibility of operation, the transport infrastructure of the data centre should support not only the technology of data networks (Ethernet, IP, etc.) but also data storage networks (FibreChannel, FCoE, iSCSI, FCIP, etc.). That is, the network infrastructure of the data centre must be convergent.

Virtualization of transport network resources to logically isolate its users or administrators from each other. In the case of creating a commercial data centre, the resources of its telecommunications infrastructure will be shared between different end users. To avoid their mutual influence on each other, it is necessary to be able to create a separate virtual data centre based on the physical.

Balancing and distributing user requests across multiple servers. To optimize the use of resources, for their flexible scaling, as well as to ensure the smooth operation of services located in the data centre, the network infrastructure must support load balancing technologies. Examples of resources that need to be balanced are Web, DNS, or Proxy servers, databases, firewalls, and more.

Discussion and conclusions

The introduction of information technology in crop management ensures:

- More exact observance of agrotechnological terms of carrying out works
- Rational use of land resources
- Reducing the number of consumables
- Improving the organization of technological works and use of equipment
- Generalization of business experience.

Investigating the features of agricultural enterprises, we can identify the following factors that affect the automation of management of the object of management:

- Significant distribution of management facilities in space, especially for large agricultural enterprises
- Poorly developed infrastructure of communication and computerization systems (insufficient number of computers in rural areas, weak radio coverage of the territory, insufficient reliability of radio communication channels)

- The need to take into account spatial factors when performing operations (geometric dimensions of the fields);
- The need to take into account spatial factors in the provision of resources (concentration of equipment and human resources in the places of operations requires time and resources)
- High cost and low quality of primary information obtained by remote sensing methods
- Some difficulties are caused by the use of sensors and other devices for collecting primary information in the field.

The rapid development of information technology used in agriculture and advances in computing and communication tools include the following problems of information quality:

- The increase in the number of mobile computing, registration, visual devices, leads to an increase in the complexity of information distribution systems and increase uncertainty, which significantly affects the quality and security of information
- The use of data on the physical condition of control objects (soil condition, crop condition, cartographic data, data on the use of agricultural machinery, etc.), as a rule, also increases the indeterminacy in time and space. This concerns the complexity of the model of the external environment in which the ARS is located and performs the tasks
- The increase in users of communication ADR creates uncertainty in the actions of users in the process of interactive interaction with information systems, which requires the use of complex models of individual user behaviour and models of collective user behaviour.

In conclusion, it should be noted that the stability of communication channels and security is largely determined by the reliability of data transmission in the network, which is provided by the design of the appropriate network structure. This in turn will enable the implementation of the first level of the concept of Cyber Situational Awareness in information technology to protect automated management systems for agricultural enterprises.

Using modern methods of protection of corporate networks, the first level of enterprise management will be aware of the real state of the object of management and cyber threats.

Acknowledgements

This research was supported by CyRADARS project (SPS G5286 “Cyber Rapid Analysis for Defence Awareness of Real-time Situation”) in the frame of the NATO Science for Peace and Security program.

References

[1] Ulrik Franke and Joel Brynielsson, “Cyber Situational Awareness: A Systematic Review of the Literature,” *Computers & Security* 46 (2014): 18-31, https://doi.org/10.1016/j.cose.2014.06.008.

[2] Kjell Hausken and Gregory Levitin, “Review of systems defense and attack models,” *International Journal of Performability Engineering* 8, no. 4 (2012): 355-366.

[3] Nancy Cooke, Michael Champion, Prashanth Rajivan, and Shree Jariwala, “Cyber Situation Awareness and Teamwork,” *EAI Endorsed Transactions on Security and Safety* 13, no. 2 (2013): e5, https://doi.org/10.4108/trans.sesa.01-06.2013.e5.

[4] Maanak Gupta, Mahmoud Abdelsalam, Sajad Khorsandroo, and Sudip Mittal, “Security and Privacy in Smart Farming: Challenges and Opportunities,” *IEEE Access* 8 (2020): 1-21, https://doi.org/10.1109/ACCESS.2020.2975142.

[5] Mica Endsley, “Toward a Theory of Situation Awareness in Dynamic Systems,” *Human Factors* 37, no. 1 (1995): 32-64, http://uwf.edu/skass/documents/HF.37.1995-Endsley-Theory_000.pdf.

[6] B. McGuinness and L. Foy “A Subjective Measure of SA: The Crew Awareness Rating Scale (CARS),” *Proc. of the First Human Performance, Situation Awareness and Automation Conference, Savannah, Georgia, 2000*.

[7] Cyril Onwubiko and Thomas Owens, “Review of Situational Awareness for Computer Network Defense,” in C. Onwubiko and T.J. Owens (eds.) *Situational Awareness in Computer Network Defense: Principles, Methods and Applications* (International Science Reference, 2011).

About the Authors

Valentyn V. **Nekhai** – Assistant of Department of information technology and software engineering, Chernihiv National University of Technology, Chernihiv, Ukraine. http://orcid.org/0000-0002-6209-5661

Mariia **Dorosh**, D.Sc., Associate professor, professor on Information Technology and Software Engineering department, Chernihiv National University of Technology, Chernihiv, Ukraine. https://orcid.org/0000-0001-6537-9857

Valentyn A. **Nekhai** – PhD in Economics, Associate Professor, doctoral student of the department of accounting, taxation and audit, Chernihiv National University of Technology, Chernihiv, Ukraine. http://orcid.org/0000-0002-9548-0961