UDC 004.7:056.5 **doi: 10.32620/reks.2022.4.04**

Ihor FURSOV, Klym YAMKOVYI, Oleksandr SHMATKO

National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine

SMART GRID AND WIND GENERATORS: AN OVERVIEW OF CYBER THREATS AND VULNERABILITIES OF POWER SUPPLY NETWORKS

The subject *of this study is the cyber vulnerability of wind generators, as part of the cyberphysical system of intelligent power supply networks, Smart Grid. Wind generators produce electricity for further distribution in the network between «smart» electricity consumers, which often include autonomous power systems in medical institutions, autonomous power supply of homes, charging stations for cars, etc. Wind generators operate in two aspects: in the physical and information space. Thus, a violation of the security of the information flow of a wind generator can affect the physical performance of electricity generation, and disable equipment.* ***The study aims*** *to identify types of cyber threats in the wind generator network based on the analysis of known attack incidents, analysis of the Smart Grid network structure, network devices, protocols, and control mechanisms of a wind generator.* ***The tasks*** *of the work are: review and analyze known cyberattack incidents; review the classification of cyber threats to wind farms; consider the most common methods of attacks on the cyber-physical system of wind farms; consider ways of intrusions into the information flow of the cyberphysical system wind generator; consider resilience mechanisms of wind generators in case of a cyberattack, consider the directions of further research. The* ***methods*** *are a systematic approach that provides a comprehensive study of the problem, quantitative and qualitative analysis of incidents of cyber attacks on wind generators, and methods of attacks. The following* ***results*** *were obtained: 11 large-scale known incidents of cyber attacks on the cyberphysical systems of the energy sector and smart power supply networks were analyzed, and information flow features and structure of the wind generators were considered. Main communication interfaces of the Smart Grid network were reviewed, control mechanisms for the physical parts of the wind generator system such as automatic voltage regulator, and automatic generation control were observed, vulnerable data transmission protocols, DNP3 in particular, were analyzed, possible consequences in the case of a cyber-intrusion into the network were considered.* ***Conclusions****: wind farms, as part of the Smart Grid system, are a convenient target for cyberattacks, as the number of potential ways to interfere with the information flow of the cyberphysical system is growing due to an increase in the number of sensors, communication channels in the network. This is especially important for the further development of wind farm security systems, which at the time, are not able to provide high accuracy of intrusion detection into the information flow.*

Keywords: *cyber threat; Smart Grid; CPS; cybersecurity; wind generators.*

Introduction

The growing number of cyber attacks on critical infrastructure facilities, due to large-scale digitalization, causes increased attention to cybersecurity of such complex intelligent systems [1–3]. Critical infrastructure includes objects, networks, services, and systems which failure will certainly affect the health, safety, and well-being of the country's citizens. The share of significant cyber attacks on critical infrastructure facilities reaches above 50% of all incidents, according to the [4].

Among other critical infrastructure facilities, wind generators becomes target of cyber attacks more often [5–6].

The approach of ensuring the security of critical infrastructure objects is based on protection of both cyber and physical components of so-called cyberphysical systems.

A cyberphysical system (CPS), which commonly used for managing the critical infrastructure objects, is a system that can effectively integrate intelligent and physical components through the major use of sensor, computing, and network technologies.

A typical conceptual scheme of a CPS system includes:

– a set of interrelated physical components that implement the technological process;

– a set of interrelated information components that manage the process to varying degrees of automation;

– a communication environment that provides information exchange within the system with the environment and transmission of control commands through a programmable logic controller by an actuator [7].

This article discusses the issues of wind farms information security. Since the number of attacks on the CPS of wind farms, smart grid systems has been steadily developing recently, the question arises of review all possible vulnerabilities and cyber threats to these systems, as well as resilience of this systems in case of an attack.

A wind generator is part of a smart power grid that converts wind energy into electricity. The wind generator is controlled by commands transmitted over the network through a large number of interfaces and network devices. Thus, the attacker gets a large set of possibilities to interfere with the information flow of the wind generator. Methods for detecting threats from wind generators include physical and informational approaches. When detecting information threats to the CPS of wind generators, a comprehensive analysis of sensor indicators is necessary, identifying indicators that would correspond to the state of normal operation or security violations. The issue of ensuring the security of wind generators is complex, multifaceted and relevant at the present time.

Objectives of the article are the following:

- to overview cyberattack incidents on Smart Grid and wind generators (Section 1);
- to classify and overview cyber threats to wind farms (Section 1);
- to consider the structure of Smart Grid of wind farms (Section 2);
- to suggest and analyse security related control mechanisms of the cyberphysical system of wind generator (Section 3);
- to consider resilience mechanisms of wind generators in case of cyberattack and discuss directions of future research (Conclusions).

1. Cyber threats of energy plants: statistic and classification

Let's look at the most significant incidents of cyber attacks on Smart grid and wind generators in recent years. According to [8] only in German several energy suppliers were hit by cyberattacks in recent months.

Table 1 lists the most significant cyber attacks on parts of Smart Grid and wind farms.

Table 1

List of large-scale cyber attacks on critical infrastructure facilities of energy sector

Year	Location	Attack objects	Type	Impact
2014	International	Energy companies	NA	For the purpose of espionage, 250 companies in the USA and Western Europe were infected [9]
2015	Ukraine	Electricity operators	DDoS	30 electricity substations disconnected from the grid, eight provinces without electricity for several hours [9]
2015	UAE	Energy companies	Trojan “Laziok”	Espionage, strategically important data theft [10]
2017	Turkey	Electric network in Istanbul	Trojan	Power system failure, blackout in the city over 2 hours [11]
2019	Utah, USA	Wind farms	Trojan	Power system failure [12]
2020	USA	Energy department	Trojan	Power system failure [13]
2021	Denmark	Wind turbines of Vestas company	Trojan	Vestas, the world’s largest supplier of wind turbines, has revealed that data has been compromised following a suspected cyber-attack on 22.11.21 [14].
2022	Ukraine	Ukranian electrical substations	Industroyer2	In April 2022 virus was discovered targetting regional high-voltage electrical substations in Ukraine. The malware has capability to directly control switches and circuit breakers using four Industrial control system (ICS) protocols. Attack was detected mitigated before a black-out occurred [15].
2022	Austria	Wind turbines of Enercon company	NA	The malfunction affected around 5,800 wind turbines across Europe, with a total output of 11,000 MW. It took several weeks until all of these turbines become controlled again [16].
2022	Germany	Wind turbines of Windtechnik company	NA	Deutsche Windtechnik has been hit by an external cyber attack on its IT systems on 12.04.22. Immediately after the attack was detected, all remote data monitoring connections to the wind turbines were disconnected for security reasons [17].
2022	Germany	Wind Turbine Giant Nordex	Bazar Loader TrickBot	The cyber-attack was detected by IT security team early. Nordex revealed that the necessary response protocols were taken and IT systems across multiple locations and business units were shut down [18].

Each of these attacks was aimed at the responsible life support system, consisted of advanced steps and was successfully carried out in the presence of developed CPS security systems, which points to insufficient security and vulnerability of such systems to hacker attacks, the need to develop an effective and flexible mechanism for detecting CPS security violations.

Fig. 1 shows distribution of cyber attacks by target sectors. Cyber attacks on energy sector ranks first on the chart with 283 incidents [19].

There are 274 attacks on critical manufacturing. This also indicates the high rate of cyber attacks on energy facilities at the time [19].

The high rate of attacks on critical infrastructure facilities is very concerning, due to impact of this objects on human lifes, and implementation on this facilities cyberphysical systems, protection issues of which are only being worked out at the moment.

The reason that energy facilities, which include «Smart Grid» (SG), power supply networks, are more often targeted by intruders, is because a successful attack on them can lead to significant financial losses, disabling equipment and at the same time affect the well-being of a numerous people. Prevention of cyber attacks on energy facilities is becoming a priority task of law enforcement agencies at the state level [20].

Cyber-incident categories can be divided to these below:

– Cyber warfare is defined as the use of cyber capabilities on a sufficient scale and over a certain period of time and at high speed in order to achieve certain goals or effects in or through cyberspace. Such actions are considered as a threat to the national interests of the state [21].

– Hacktivism is a form of nonviolent digital activism, where the motive is to achieve political, social or religious justice in accordance with the goals of the group [22].

– Cybercrime is a socially dangerous guilty act committed in cyberspace with the usage of electronic computers (computers), automated systems, computer networks or telecommunication networks, which consists in illegal, unauthorized creation, storage, processing, forgery, blocking, destruction of infrastructure objects technical information [23].

Fig. 2 shows classification of SG cyber threats.

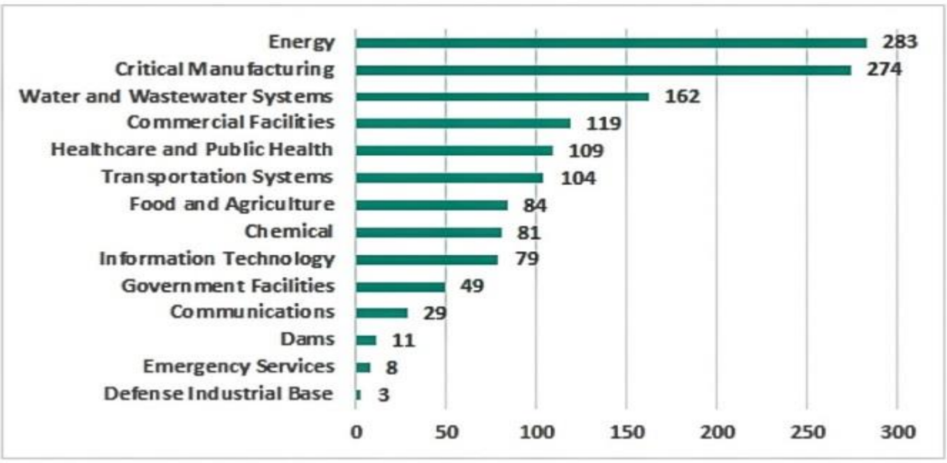

Fig. 1. Cyber-attacks incidents by target sectors (Data from ICS-CERT 2019) [19]

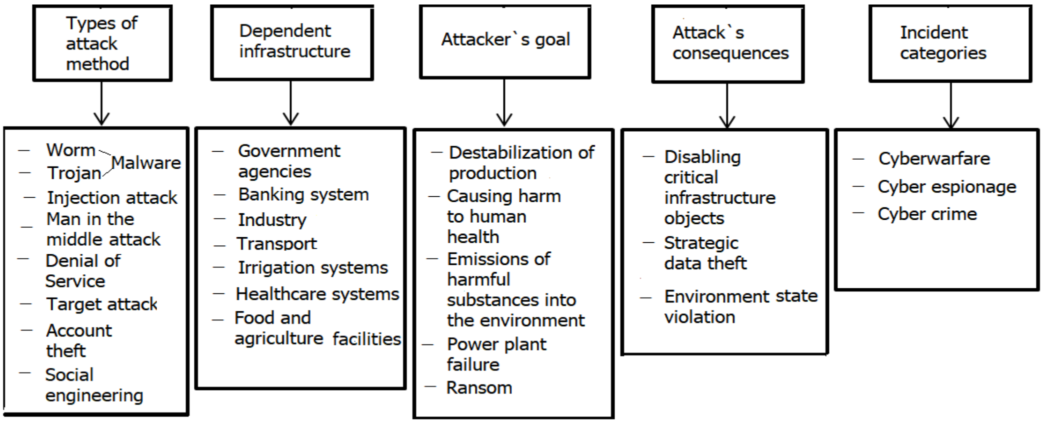

Fig. 2. Cyber threats classification

Below a brief description of those shown in fig. 2, common types of attacks on wind farms, is given.

1. Worm virus: all mechanisms of worm virus are divided into two large groups:

– Exploiting vulnerabilities and administrative errors in the software installed on target’s computer. As an example, the Morris worm used known vulnerabilities in software at that time, namely in the sendmail mail server, the finger service, and selected a password from a dictionary. Such worms are able to spread independently, selecting and attacking computers in fully automatic mode [24].

– Using of so-called social engineering, so the user himself provokes the launch of malware. To convince the user that the file is safe, attacker can exploit flaws in the program's user interface.

2. Trojan virus: this is a type of program that adds subversive functionality to link to an existing program. A Trojan is malicious software that hides the true purpose of its activities by masking it. This type is not able to copy or infect files on its own. To get into the victim's device, the threat uses other means, such as hidden downloading, exploiting vulnerabilities, downloading other malicious code, or social engineering methods [25].

3. Injection attack allows an attacker to inject code into a program or query or inject malware onto a computer in order to execute remote commands that can read or modify a database, or change data on a remote device. The common types of injection attack are: Blind SQL Injection, Blind XPath Injection, Format String Attack, SQL Injection, SSI Injection [26].

4. A man-in-the-middle attack (MitM attack) refers to the method where a hacker intercepts the data traffic between two communication partners, leaving both parties to think that they are only communicating with each other. These kinds of attacks were previously carried out by manipulating physical communication channels. MitM attacks are primarily seen in computer networks where there is an attempt to overturn Secure Sockets Layer (SSL) encryptions with the aim of obtaining secret information, usernames, passwords, or bank details. The basic course of a man-in-the-middle attack is as follows: System A attempts to establish an encrypted connection with System B. Instead, the data flow is redirected by a criminal third party, which results in the encrypted connection running from system A to system C and only then is it redirected to System B. This means that the one in control of System C (usually the attacker) can see the data traffic in its entirety, record it, or manipulate it [27].

5. Denial of Service: defined as an attack that aims to disable the network or computer from providing normal services. It is assumed that this happens only when access to the computer's network or resource is intentionally disrupted or blocked due to malicious actions of another user. A denial-of-service attack overwhelms systems, servers, or networks with traffic, resulting in resource and bandwidth depletion. As a result, the system loses the ability to perform normal requests. Hackers can also use compromised devices to organize attacks. This type of attack is called a distributed denial-of-service attack (DDoS attack) [28].

6. Targeted attack: represents a malicious attack targeting a specific person, software, system, or company. It can be used to extract information, disrupt operations, or destroy a specific type of data on the target machine.

7. Account theft: defined as the process by which hackers steal a physical device with data, email, or other account of a particular person associated with a service or computing device. One of the tactics of cybercriminals to steal accounts is phishing campaigns. Typically, hackers send an email with a link that redirects the user to a website that looks the same as a popular social network such as Twitter, with a window to log in to the social network. Without even suspecting that this is a fake page, the user tries to log in to the account, but in fact the login data is stolen by intruders. Having gained access to the account, fraudsters can receive and send confidential data about the operation of distributed cyberphysical systems, manage individual production operations, which leads to a security violation of the entire system and the need to identify and eliminate the negative consequences of an attack. The first sign of account hacking is blocking the login and the need to re-log in to the account on all devices [29].

Many attacks on cyberphysical systems involve replacing information flow data in order to simulate the normal operation of the system with subsequent incorrect operation of installations. This leads to a delayed response to an error in the system, loss of control over parts of the system, and the initiative of further actions of the attacker.

The list of smart grid power dependent sectors is given below:

– government: refers to local or national government bodies, including buildings/housing, emergency services, public benefits and Social Services, federal and state governments;

– a banking system refers to a network of institutions that provides financial services to the people. The following are some of the institutions that belong to the banking system: central banks, commercial banks, internet banks, investment banks, savings and loan associations, insurance companies, and credit unions. The purpose of banking systems is to provide security and confidence in the economy [30];

– industry: these are industries that consist of all the equipment used to produce, process, or collect goods;

– private institutions: refers to a part of a country's organization run by individuals and companies, not the government;

– critical infrastructure objects are organizations and institutions whose functioning ensures the life of a large number of people. These objects include power plants, irrigation networks, data transmission networks, digitally visible medical institutions, etc.. The functioning of critical infrastructure facilities is usually provided by cyberphysical systems;

– irrigation systems include purification and irrigation subsystems maintain the necessary quality of fresh water for the needs of urban residents and the needs of the agricultural sphere [31]. Cyber attack on CPS of water system can affect the harvest and also cause, for example, food poisoning;

– healthcare CPS frequently becomes a target to cybercriminals. In this case, aim is to achieve personal data of patients and possibly change sensor data for incorrect treatment.

The energy sector is remarkable because smart grid networks are included in the energy supply of a number of the above-listed objects of critical infrasctucture, including irrigation stations, plants, transport, smart healthcare systems, etc.

2. Structure of Smart Grid and wind generators

In general, «Smart Grid» is considered as modernized power supply networks that use information and commuication technologies to collect information about electricity production and energy consumption, and can automaticly increase the efficiency, reliability, economic benefits of electricity production and distribution [32]. Smart wind farms are part of smart power supply networks SG. This type of power plant is a network of wind towers located in an area with permanent wind flows, and converts wind energy into alternating electric current energy by transmitting the torque of the generator blades to the generator rotor units. SG provides reliable data communication system, sensors and advanced meter technologies, cyber security devices, end user devices, and sophisticated energy management system based on energy availability and demand optimization [33]. Towers are located mainly in coastal and mountainous areas. A tower, its height, the size of the blades, and the ability to adjust the angle of the tower during operation should be considered in order to achieve more power production. The CPS of the wind generator is designed to accumulate the generated electrical energy, adjust the optimal parameters of the tower operation to perform optimal installation efficiency, as well as distribute electricity taking into account the individual needs of consumers. Consumers of electricity from Smart Grid power plants are primarily automated control systems such as "smart" homes, car charging stations, autonomous power supply systems for administrative buildings: hospitals, educational institutions, etc.. Thus, failures, violations of the information security of the CPS of wind power plants can lead to huge economic losses, threats to human life as a result of disconnection of electricity supplies from important support systems operating from the power grid.

An example of a successful cyberattack on wind farms is the incident with the disconnection of ten wind generators from the main power supply network in Utah, USA, which occurred in the spring of 2019. The attackers used the mechanism of frequent requests to parts of the CPS of the wind farm, which led to a shutdown of the supply of 500 MW of electricity. To achieve criminal goals, vulnerabilities in the security mechanisms of networks manufactured by Cisco were used. The presence of system failures was detected late, which led to significant financial losses [34].

Complex information management systems have vulnerabilities to carry out a cyber attack on the CPS of the electric network. Classification of cyber attacks by the attack’s target is given below:

– targeted on components: electronic devices, remote terminals (RTU), or human-machine interface terminals (HMI) [35] usually have a dedicated interface for remote configuration. Through this type of access, a hacker can intercept control of the device and cause incorrect operation of the entire system, for example, falsify the transmitted data to the operator, complete or partial failure of the device;

– targeted on protocols: the ease of understanding the principles of operation and documentation of modern data transmission protocols, such as distributed network protocol 3 (DNP3), which is common in European electrical network management systems, makes it easy to perform attacks on the CPS. Cyber criminal can send falsified data, which leads to financial losses due to excessive power generation, and danger to the lives of employees, for example, when the Power Line current is turned on if there are personnel there, to damage to equipment;

– targeted on topology: attackers can exploit vulnerabilities in the location of individual nodes in the CPS sensor network. For example, sending large volumes of requests to remote terminals creates delays in sending messages in real time. This leads to a distorted representation of the state of the environment or system components for the operator, which can lead to erroneous decisions.

It is necessary to consider the problems of cybersecurity of "smart" power supply networks in the context of analyzing the simplified SG model, taking into account information and communication technologies and data exchange interfaces at different levels of the model. Fig. 3 shows a SG model consisting of five subdomains, which are represented at three conceptual levels: services/applications, communications, and hardware. Based on research [36], general structure of the "Smart grid" network is given in fig. 3.

Fig. 3 also shows five interfaces of interaction between domains, indicated by the numbers 1-5. The characteristics of data exchange interfaces between domains of the SG network are given below:

Interface 1 – provides information exchange between power generation devices and communication networks, RTU's and power controllers [37]. Thus, energy management, control over power generation units are established. This interface transmits information about power generation, measure devices.

Interface 2 – connects the subdomain of measuring devices and the communication network (telecom operator), and allows to exchange measurement information, through the telecom operator, with service providers.

Interface 3 – formed between the customer subdomain and the communication network, and provide interaction between telecom operators and customers.

Interface 4 – this interface between the subdomain of service providers and the communication network. It provides communication services within the subdomain of service providers, in order to manage other domains.

Interface 5 – connects a subdomain of measuring instruments and a customer subdomain, providing interaction between measuring instruments and user equipment.

Each of the interfaces shown on fig.3 can become a potential target for attackers whose goal is to interfere with the information exchange of the CPS system and cause erroneous system reactions due to the presence of misinformation in the CPS information flow. The development of a universal and effective method for detecting CPS security violations becomes a top priority for designing this class of systems.CPS

The CPS of wind farms uses two-way information flow, intelligent calculations and protected communication technologies, but the presence of a huge number of sensors, many possibilities of hacking the system creates increased requirements for the security of the information flow and the state of the parameters of both equipment and the environment [36]. Thus, we have an array of data coming from a wind generator and including indicators of wind speed at several levels, ambient air temperature, temperature of the generator's operating zone, and power generated over a certain time interval.

This data set becomes a potential target of cyber criminals, in case of intrusion into system.

In the case of attack, system should have special methods for mitigating the consecuences. Targeted elements should be disconnected from the network, any potential data spread through the system should be avoid.

Possible algorithm of the attacker's action:

– an attacker interfered in the network with the help of malware or physical interception of electricity production equipment at communication and production domains;

– mechanisms for blocking the operation of the wind generator are applied;

– forward instructions are sent to telecom operators or market. After this, consumer experience outages, blackout, etc. [38].

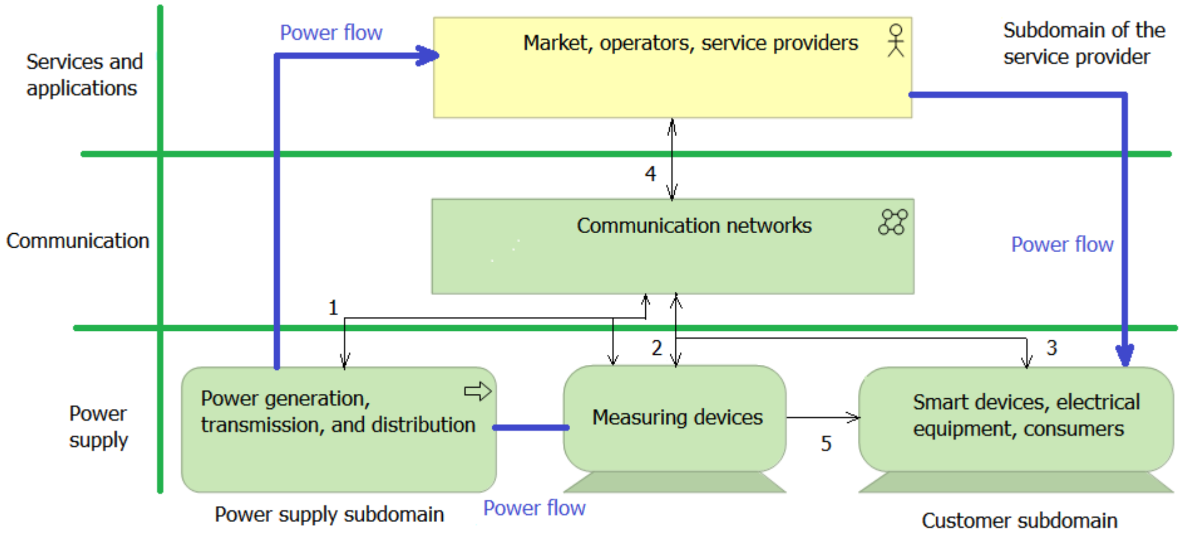
Services and applications
Power flow
Market, operators, service providers
Subdomain of the service provider
4
Communication
Communication networks
Power flow
1
2
3
Power supply
Power generation, transmission, and distribution
Measuring devices
Smart devices, electrical equipment, consumers
5
Power supply subdomain
Power flow
Customer subdomain

Fig. 3. Domain structure of "smart" power grid [36]

3. Model of attack on wind generator: ways of attack and consequences

Table 2 describes methods of attack which cyber criminal could apply to a wind farm generator. Some of them can be carried out with information flow changes, which leads a system to power loss, instability, inaccurate distribution of electric power etc. According to the late researches, such as [39], there are several network nodes, as HMI, PLC, which can be used as malware entry point.

Table 3, compiled on the basis of the research [40], contains more details on the control mechanism of the wind generator network with a description of network protocols, domains of interaction mechanisms of network devices.

Table 2

Consequences of cyber attack on wind systems [39]

Wind generator (WG) manipulation	WG controls manipulated to reduce output power.
	WG controls manipulated to increase output power.
	WG controls manipulated to continuously or harmonically adjust power output.
	WG controls manipulated to cause physical damage to turbine or connected equipment.
Communication infrastructure distortion	Impacts to normal operation of turbines, scalability of access restriction to control centers of wind plants can all beaffected by disruption of wired, wireless, and cellular communications. Communications that could be distorted, interrupted, or blocked include those between turbines and a control center and those between a wind plant network and remote-control center (potentially over Wide Area Network [WAN]).
Data falsification leading to miscoordination	Falsified field measurements could lead to misoperating of automomus subsistems of grid. Systems that could be distorted include condition-monitoring systems, structure health-monitoring systems (SHMs), SCADA units, and remote monitoring and secure access.
Internal turbine communication	Widely adapted protocol, EtherCAT, based on traditional MAC/PHY layers, is subject to attacks like MAC spoofing.
	Wireless communication applied to sending and receiving information between base and nacelle or base and remote SCADA.

Table 3

Elements of control mechanism in the power grid [40]

Observable physical parameter	Control device	Data acquisition	Network devices applied
Terminal voltage	Automatic voltage regulator	Local measurement from terminal	Single board computer PLC FPGA
Rotor speed	Governor control	Local measurement from rotor speed sensor	
Frequency	Automatic generation control	Wide-area communication (IEC 61850)	
Power generation	Security-constrained economic dispatch	Wide-area communication (IEC 61850)	
Power generation	State estimation	Wide-area communication (IEC 61850)	SCADA Historian server HMI Switch
Voltage	VAR compensation	Local measurement	
DC voltage and current	HVDC transmission control	Local measurement	
Load scheduling	Demand side management	Power demand request	Switch VPN Secondary historian
Load connected to system	Load shedding	Local frequency measurement and generation level from control center	
Consumer load	Advanced metering infrastructure	NA	

The table above lists the ways to control the devices of the wind generator system.

Wind farms often feature the same equipment and equipment configurations deployed throughout the site, or multiple sites including field devices (PLCs, RTUs, HMIs), engineering workstations and operating systems, and networking equipment. This means that, if an exploitable vulnerability is discovered affecting a device used in a wind turbine or wind plant network, it is possible that an entire plant, SCADA network, and control network could be similarly exploited with greater ease than a site employing greater device variety and device configuration. There are some knows incidents in which hackers gains control and changed important settings in automatic voltage regulator, from "automatic" to "manual". Wind plant usually operate as a single installation, all connected to the control system. Such manipulating the controls could also negatively impact stable power generation [40].

In the following table 4 we considered some of the main stages resilience of wind generators in case of potential cyber attack.

The concept of resilience is multifaceted and includes a wide range of system properties that determine the stability of the system and ability to resist cyber threats.

Table 4

Wind generator cyber-attack resilience

Resilience stage	Description
Risk assessment	Attacks modeling: – intrusion scheme should be considered, according to known cyber attack approaches; – all possible system states during the attack should be reviewed; – in the case of cyber-attack, outages should be described. Vulnerability evaluation: – protocol vulnerabilities should be reviewed; – potential vulnerabilities of generators components should be considered; – personnel accounts vulnerability should be reviewed.
Prevention	Physical security measures: – –all data in the network information flow should be encrypted; – –methods based on neural network could be applied to early detect anomaly. Data analysis approaches: In [41] a general model of the functioning of information communication systems is proposed, taking into account various groups of reasons for failures, among which is: defects or obsolescence of software, physical defects of equipment, vandal attacks, failures caused by cyber-attacks. Thus, the need for clustering of failure types is determined, and adaptability to failures is a necessary condition for ensuring the resilience of information system at Prevention stage..
Detection	Intrusion detection: – the Markov model allows us to estimate the state of the system and individual nodes of the system [42]. The author notes that to assess the level of functional security (FS) it is very convenient to use the sum of the probabilities of the system nodes being in working states according IEC 61508 standard; – complex malware detection algorithm, should be applied to the information flow, based on data flow analysis, which may include: Neural network method [43], Kalman filter method [44], Statistic methods [45]. By combination of these methods, increase in cyber-attack detection should be expected.
Mitigation	After attack, the system may require significant reconfiguration, depending on which components were affected by the cyber-attack and to what extent. System nodes should be ranged by the state estimation. System should include methods to prevent the spread of attack impacts. Applying a variety of data recovery methods, services, and services that have been affected by a cyber-attack [46]. After possible attack occurring, followed step must be performed to achieve: – network devices and facility objects under attack should be disconnected from network using safe and efficient approaches; – power outages should be avoid; – system state during cyber-attack should be deeply analyzed.

Conclusions

The active implementation of information control systems in critical infrastructure facilities, wind farms, leads to increase in the number of cyber attacks on such hybrid intelligent systems. The goal of attackers is to destabilize the work of the CPS by replacing system or sensor's data with further inadequate response of the system, which closely interacts with production processes and the environment.

As a result, the failure of the CPS directly leads not only to financial losses, but also threats the human life and threats to the environment. Cyber attacks on wind farms can cause sudden power outages to a number of smart devices: smart home systems, charging power plants for electric cars, and autonomous power supply systems in hospitals. The purpose of this paper was to review cyber threats and vulnerabilities of cyber-physical systems of wind farms.

As a result of performing the main tasks of the work, the following results were obtained:

1. A list of significant cyber attacks on the CPS of the power plants, including wind farms, is given.

2. The number of attacks on the CPS of critical infrastructure objects is analyzed. According to research results, the share of cyber attacks on CPS of energy production is above 50 %.

3. The main methods of violations of information security of the CPS were analyzed. The most common methods of attacking CPS objects of critical infrastructure objects include computer viruses Trojan, Warm, and physical hacking of CPS nodes.

4. The main vulnerabilities of the wind farm CPS are analyzed. The classification of attacks by the target of the attack and possible ways for a hacker to access the CPS's information flow are given:

– targeted components - access to the information flow via electronic devices, remote terminals (RTU) or human-machine interface (HMI) terminals;

– targeted protocols-access to the information flow via data transfer protocols, such as DNP3, allows an attacker to remotely control the state of the CPS information flow;

– targeted topology: attackers can exploit vulnerabilities in the location of individual nodes in the CPS sensor network.

4. The scheme of functioning of the "smart" power grid is analyzed. A list and description of data exchange interfaces between subdomains of smart power grid systems and wind farms is provided.

5. Attack resilience scheme of wind generators was proposed.

6. The relevance of further research on the issue of ensuring the protection of CPS of wind generators is justified.

Most of the cyber-attacks incidents on wind generators, was fulfilled with exploition of Trojan malware, phishing methods, account theft. Internal intrusion to the unprotected physical network devices also occured. A notice was made, that problem of cybersecurity of wind generators becomes more multifaceted, complicated and there is high risk of cyber-attack on wind farms CPS as it utilize standard methods for data transmittion, vulnerable protocols, such as DNP3, unprotected network devices, such switches, PLC [44].

The following future research directions are important, in our opinion:

– additional studies are needed regarding the effectiveness of the Kalman-filter, neural network, and statistical methods to identify the most efficient approach to detect cyber attacks;

– variations of considered methods can be investigated as well, because combination of these methods may be more efficient;

– cyber resilience of wind generators should be deeply considered including the development of model for analysis of system recovery after attack.

Contribution of authors: suggestion for the purpose, general structure of the work, overview of information sources on types of attacks on wind generators, classification of attacks, description of dependent critical infrastructure – **Oleksandr Shmatko**; compilation of a list of known cyber-attacks on Smart Grid, wind generators, literature review on the Smart Grid structure organization, review of Smart Grid network equipment that becomes the target of attacks by cybercriminals – **Klym Yamkovyi**; review of possible actions of intruders, review of Smart Grid control mechanisms, review of resilience scheme of the wind generator system, review of models for evaluating, detecting, mitigating the system in the case of cyber-attack, considering the course of future research, compose and prepare article for submitting – **Ihor Fursov**.

All the authors have read and agreed to he published version of the manuscript.

References (GOST 7.1:2006)

1. Gadre, M. Industry 4.0 - Digital Transformation, Challenges and Benefits [Text] / M. Gadre, A. Deoskar // International Journal of Future Generation Communication and Networking. – 2020. – Vol. 13, No. 2. – P. 139 – 149.

2. Technique for IoT malware detection based on control flow graph analysis [Text] / K. Bobrovnikova, S.

Lysenko, B. Savenko, P. Gaj, O. Savenko // Radioelectronic and Computer Systems. – 2022. – No. 1. – P. 141 – 153. DOI: 10.32620/reks.2022.1.11

3. Bi, W. Profit-Oriented False Data Injection Attack Against Wind Farms and Countermeasures [Text] / W. Bi, G. Chen, K. Zhang // IEEE Systems Journal. – 2022. – Vol. 16, No. 3. – P. 3700-3710. DOI: 10.1109/JSYST.2021.3107910.

4. Cybersecurity Guide for Distributed Wind 2021 [Electronic resource] / M. Culler, B. Smith, F. Cleveland, S. Morash, J. Gentle. – Access mode: https://resilience.inl.gov/wp-content/uploads/2021/11/ 21-50152_CG_for_DW_R5.pdf (Accessed: 02 Jun. 2022).

5. Cyber-Physical System (CPS) Application - A REVIEW [Text] / S. Raisin, J. Jamaludin, F. Jamal, N. Hazwani, S. Zaini, B. Naeem // Reka elkomika: Jurnal Pengabdian kepada Masyarakat. – 2020. – Vol. 1, No. 2. – P. 52-65. DOI: 10.26760/rekaelkomika. v1i2.52-65

6. Passeri, P. April 2021 Cyber Attack Statistics. May 12, 2021 [Electronic resource] / P. Passeri. – Access mode: https://www.hackmageddon.com/2021/ 05/12/april-2021-cyber-attacks-statistics/. – 02 Jun. 2022.

7. Голембо, В., Бочкарьов, О. Підходи до побудови концептуальних моделей кіберфізичних систем [Текст] / В. Голембо, О. Бочкарьов // Видавництво Національного університету “Львівська політехніка”. – 2017. – № 1(868). – С. 168-178.

8. Major Cyber Attacks in Review: June 2022 [Electronic resource]. – Access mode: https://socradar. io/major-cyber-attacks-in-review-june-2022/. – 09 Jun 2022.

9. Desarnaud, G. Cyber Attacks and Energy Infrastructures: Anticipating Risks [Electronic resource] / G. Desarnaud. – Access mode: https://www.ifri.org/en/ publications/etudes-de-lifri/cyber-attacks-and-energy-infrastructures-anticipating-risks. (accessed: 02 Jun. 2022).

10. Millman, R. Energy companies targeted by Laziok Trojan [Electronic resource] / R. Millman. – Access mode: https://www.itpro.co.uk/security/24338/ energy-companies-targeted-by-laziok-trojan. – 02 Jun. 2022.

11. Paganini, P. Recent power outages in Turkey were also caused by cyber attacks [Electronic resource] / P. Paganini. – Access mode: https://securityaffairs.co/ word press/55176/hacking/power-outages-turkey.html. – 03 Jun. 2022.

12. Sobczak, B. First-of-a-kind U.S. grid cyberattack hit wind, solar [Electronic resource] / B. Sobczak. – Access mode: https://www.wind-watch.org/news/ 2019/11/02/first-of-a-kind-u-s-grid-cyberattack-hit-wind-solar/. – 03 Jun. 2022.

13. Collier, K. Energy Department says it was hacked in suspected Russian campaign [Electronic resource] / K. Collier, L. Strickler. – Access mode: https://www.nbcnews.com/news/usnews/department-energy-says-it-was-hacked-suspected-russian-campaign-n1251630. – 03 Jun. 2022.

14. Bannister, A. Wind turbine giant Vestas confirms data breach following ‘cybersecurity incident’ [Electronic resource] / A. Bannister. – Access mode: https://portswigger.net/daily-swig/wind-turbine-giant-vestas-confirms-data-breach-following-cybersecurity-incident. – 03 Jun. 2022.

15. Cyber Attacks on the Power Grid. Industroyer2 [Electronic resource]. – Access mode: https://securityboulevard.com/2022/05/cyber-attacks-on-the-power-grid/. – 04 Jun. 2022.

16. Akoto, P. Enercon: Thousands of wind turbines need new hardware [Electronic resource] / P. Akoto. – Access mode: https://www.energate-messenger.com/ news/220914/enercon-thousands-of-wind-turbines-need-new-hardware. – 04 Jun. 2022.

17. Deutsche Windtechnik hit by cyber attack [Electronic resource]. – Access mode: https://renews. biz/77220/ deutsche-windtechnik-hit-by-cyber-attack/. – 04 Jun. 2022.

18. David, B. Wind Turbine Giant Nordex Hit By Cyber-Attack [Electronic resource] / B. David. – Access mode: https://www.infosecurity-magazine.com/ news/wind-turbine-nordex-cyber-attack/#:~:text= German%20wind%20turbine%20manufacturer %2C%20Nordex%20Group%2C%20was%20hit,to%20 Nordex%2C%20and%20response%20measures%20were%20taken%20quickly. – 03 Jun. 2022.

19. Threat landscape for industrial automation systems. Vulnerabilities identified in 2019 [Electronic resource]. – Access mode: https://icscert.kaspersky. com/publications/reports/2020/04/24/threat-landscape-for-industrial-automation-systems-vulnerabilities-identified-in-2019/. – 04 Jun. 2022.

20. Cyber-Physical Stress-Testing Platform for Water Distribution Networks [Text] / D. Nikolopoulos, G. Moraitis, D. Bouziotas, A. Lykou, G. Karavokiros, C. Makropoulos // Journal of Environmental Engineering. – 2020. – Vol. 146, no. 7. – 22 p. DOI: 10.1061/(ASCE)EE.1943-7870.0001722.

21. Камчатний, М. В. Основні ознаки поняття ”кібервійна” у сучасному міжнародному праві [Текст] / М. В. Камчатний // Альманах міжнародного права. – 2017. – № 15. – С. 12 – 22.

22. Что такое Хактивизм? Кампании, которые сформировали движение [Електронний ресурс]. – Режим доступа: https://www.securitylab.ru/blog/ company/PandaSecurityRus/348956.php. – 03 Jun. 2022.

23. Кримінальна відповідальність за кіберзлочини [Електронний ресурс]. – Режим доступу: https://wiki.legalaid.gov.ua/index.php/ Кримінальна_відповідальність_за_кіберзлочини. – 03 Jun. 2022.

24. What is the Morris worm? History and modern impact. Available at: https://www.okta.com/uk/identity-101/morris-worm/ – 03 Jun 2022.

25. Енциклопедія загроз ESET. Що таке троян? [Електронний ресурс]. – Режим доступу:

https://www.eset.com/ua/support/information/entsiklopediya-ugroz/troyan/. – 03 Jun. 2022.

26. Injection attacks [Electronic resource]. – Access mode:https://www.ibm.com/docs/en/snips/4.6.0?topic=categories-injection-attacks. – 04 Jun. 2022.

27. What is a man-in-the-middle-attack? [Electronic resource]. – Access mode: https://www.ionos.com/digitalguide/server/security/man-in-the-middle-attack-an-overview-of-attack-patterns/. – 04 Jun. 2022.

28. Alotaibi, F. Matrix profile for DDoS attacks detection [Text] / F. Alotaibi, A. Lisitsa // Proceedings of the 16th Conference on Computer Science and Intelligence Systems, September 2–5. – 2021. ACSIS. – Vol. 25. – P. 357-361. DOI: 10.15439/2021F114.

29. Фахівці з кіберзахисту розповіли про ознаки злому акаунтів в соцмережах [Електронний ресурс]. – Режим доступу: https://www.unian.ua/science/10963961-fahivci-z-kiberzahistu-rozpovili-pro-oznaki-zlomu-akauntiv-v-socmerezhah.html. – 04 Jun. 2022.

30. Lee, K. Banking Systems, Types and Components [Electronic resource] / K. Lee, B. Whiting. – Access mode: https://study.com/academy/lesson/banking-system-definition-types.html. – 04 Jun. 2022.

31. Femi, J. G. Smart Water Management System [Text] / J. G. Femi // International Journal of Smart Sensor and Adhoc Network. – 2022. – Vol. 3, No. 2. – P. 9-16. DOI: 10.47893/IJSSAN.2022.1213.

32. Костров, Д. "Умные сети электроснабжения" (smart grid) и проблемы с кибербезопасностью [Електронний ресурс] / Д. Костров. – Режим доступу: https://lib.itsec.ru/articles2/in-ch-sec/umnye-seti-elektrosnabzheniya-smart-grid-i-problemy-s-kiberbezopasnostyu. – 04 Jun. 2022.

33. Survey of Smart Grid Concepts and Technological Demonstrations Worldwide Emphasizing on the Oman Perspective [Text]/ A. H. Al-Badi, R. Ahshan, N. Hosseinzadeh, R. Ghorbani, E. Hossain // Applied System Innovation. – 2020. – Vol. 3, No. 1. – 27 p. DOI: 10.3390/asi3010005.

34. Goud, N. Utah Wind and Solar Power Generation hit by a Cyber Attack [Electronic resource] / N. Goud. – Access mode: https://www.cybersecurity-insiders.com/utah-wind-and-solar-power-generation-hit-by-a-cyber-attack/. – 05 Jun. 2022.

35. Young, S. N. Review of Human–Machine Interfaces for Small Unmanned Systems With Robotic Manipulators [Text] / S. N. Young, J. M. Peschel // IEEE Transactions on Human-Machine Systems. – 2020. – Vol. 50, No. 2. – P. 131-143. DOI: 10.1109/THMS.2020.2969380.

36. Abrahamsen, F. E. Communication Technologies for Smart Grid: A Comprehensive Survey [Text] / F. E. Abrahamsen, Y. Ai, M. Cheffena // Sensors. – 2021. – Vol. 21, No. 23. – 24 p. DOI: 10.3390/s21238087.

37. etap iCE™ - Intelligent Control Enterprise Hardware [Electronic resource]. – Access mode: https://etap.com/product/etapiCE-DAC-Hardware. – 05 Jun. 2022.

38. Brief Survey on Attack Detection Method for Cyber-Physical Systems [Text] / S. Tan, J. Guerrero, P. Xie et al. // IEEE Systems Journal. – 2020. – Vol. 14, no. 4. – P. 5329-5339. DOI: 10.1109/JSYST.2020.2991258.

39. Roadmap for Wind Cybersecurity. U.S. Department of Energy (DOE) Energy Efficiency and Renewable Energy (EERE) [Text]. – Wind Energy Technologies Office, 2020. – 84 p.

40. Cyber-Physical Power System (CPPS): A Review on Modeling, Simulation, and Analysis With Cyber Security Applications [Text] / R. V. Yohanandhan, R. Elavarasan, O. Manoharan, I. Mihet-Popa // IEEE Access. – 2020. – Vol.8. – P. 151019-151064. DOI: 10.1109/ACCESS.2020.3016826.

41. Поночовний, Ю. Л. Методологія забезпечення гарантоздатності інформаційно-керуючих систем з використанням багатоцільових стратегій обслуговування [Текст] / Ю. Л. Поночовний, В. С. Харченко // Радіоелектронні і комп'ютерні системи. – 2020. – № 3(95). – С. 43-58. DOI: 10.32620/reks.2020.3.05.

42. Одарущенко, О. М. Марковські моделі оцінювання функціональної безпеки програмно-технічних комплексів на самодіагностовних програмовних платформах з урахуванням помилок засобів контролю [Текст] / О. М. Одарущенко, О. Б. Одарущенко, В. С. Харченко // Радіоелектронні і комп'ютерні системи. – 2019. – № 4(92). – С. 17-29. DOI: 10.32620/reks.2019.4.02.

43. Attack Detection and Localization in Smart Grid with Image-based Deep Learning [Text] / M. Mohammadpourfard, I. Genc, S. Lakshminarayana and C. Konstantinou // 2021 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm). – 2021. – P. 121-126. DOI: 10.1109/SmartGridComm51999.2021.9631994.

44. State Estimation within IED Based Smart Grid Using Kalman Estimates [Text] / M. Rashed, I. Gondal, J. Kamruzzaman, S. Islam // Electronics. – 2021. – Vol. 10, no. 15. – Article no. 1783. – 6 p. DOI: 10.3390/electronics10151783.

45. Фурсов, І. І., Шматко, О. В. Аналіз статистичних показників дисперсії, асиметрії та ексцесу при визначенні порушень інформаційної безпеки кіберфізичних систем вітрових генераторів [Текст] / І. І. Фурсов, О. В. Шматко // Радіоелектронні і комп'ютерні системи. – 2021. – No. 4. – С. 132-144. DOI: 10.32620/reks.2021.4.11.

46. Резильєнтність комп'ютерних систем в умовах кіберзагроз: таксономія та онтологія [Текст] / С. М. Лисенко, В. С. Харченко, К. Ю. Бобровнікова, Р. В. Щука // Радіоелектронні і комп'ютерні системи. – 2020. – № 1(93). – С. 17-28. DOI: 10.32620/reks.2020.1.02.

47. Software Defined Networks-Based Smart Grid Communication: A Comprehensive Survey [Text] / M. H. Rehmani, A. Davy, B. Jennings, C. Assi // IEEE Communications Surveys & Tutorials. – 2019. – Vol.

21, iss. 3. – P. 2637-2670. DOI: 10.1109/COMST.2019.2908266.

48. Study of Smart Grid communication network architectures and technologies [Text] / N. Raza, Q. M. Akbar, A. A. Soofi, S. Akbar // Journal of Computer and Communications. – 2019. – Vol. 7. No. 3. – P. 19-29. DOI: 10.4236/jcc.2019.73003.

References (BSI)

1. Gadre, M., Deoskar, A. Industry 4.0 - Digital Transformation, Challenges and Benefits. *International Journal of Future Generation Communication and Networking*, 2020, vol. 13, no. 2, pp. 139-149.

2. Bobrovnikova, K., Lysenko, S., Savenko, B., Gaj, P., Savenko, O. Technique for IoT malware detection based on control flow graph analysis. *Radioelectronic and Computer Systems*, 2022, vol. 1, no. 11, pp. 141-153. DOI: 10.32620/reks.2022.1.11.

3. Bi, W., Chen, G. and Zhang, K. Profit-Oriented False Data Injection Attack Against Wind Farms and Countermeasures. *IEEE Systems Journal*, 2022, vol. 16, no. 3, pp. 3700-3710. DOI: 10.1109/JSYST.2021.3107910.

4. Culler, M., Smith, B., Cleveland, F., Morash, S., Gentle, J. *Cybersecurity Guide for Distributed Wind 2021*. Available at: https://resilience.inl.gov/wp-content/uploads/2021/11/21-50152_CG_for_DW_R5.pdf (accessed: 02 Jun. 2022).

5. Raisin, S., Jamaludin, J., Rahalim, F., Jamal, F., Hazwani, N., Zaini, S., Naeem, B. Cyber-Physical System (CPS) Application - A REVIEW. *Reka elkomika: Jurnal Pengabdian kepada Masyarakat*, 2020, vol. 1, no. 2, pp. 52-65. DOI: 10.26760/rekaelkomika.v1i2.52-65.

6. Passeri, P. *April 2021 Cyber Attack Statistics*. Available at: https://www.hackmageddon.com/2021/05/12/april-2021-cyber-attacks-statistics/ (accessed: 02 Jun. 2022).

7. Holembo, V., Bochkar'ov, O. Pidkhody do pobudovy kontseptual'nykh modeley kiberfizychnykh system [Approaches to the construction of conceptual models of cyberphysical systems]. *Publishing house of the "Lviv Polytechnic" National University*, 2017, no. 1, pp. 168-178.

8. *Major Cyber Attacks in Review: June 2022*. Available at: https://socradar.io/major-cyber-attacks-in-review-june-2022/. (accessed: 02 Jun. 2022).

9. Desarnaud, G. *Cyber Attacks and Energy Infrastructures*: *Anticipating Risks*, Etudes de l'Ifri. Available at: https://www.ifri.org/en/publications/etudes-de-lifri/cyber-attacks-and-energy-infrastructures-anticipating-risks. (accessed: 02 Jun. 2022).

10. Millman, R., *Energy companies targeted by Laziok Trojan*. Available at: https://www.itpro.co.uk/security/24338/energy-companies-targeted-by-laziok-trojan. (accessed: 02 Jun. 2022).

11. Paganini, P. *Recent power outages in Turkey were also caused by cyber attacks*. Available at: https://securityaffairs.co/wordpress/55176/hacking/power-outages-turkey.html. (accessed: 03 Jun. 2022).

12. Sobczak, B. *First-of-a-kind U.S. grid cyberattack hit wind, solar*. Available at: https://www.windwatch.org/news/2019/11/02/first-of-a-kind-u-s-grid-cyberattack-hit-wind-solar/. (accessed: 03 Jun. 2022).

13. Collier, K., Strickler, L. *Energy Department says it was hacked in suspected Russian campaign*. Available at: https://www.nbcnews.com/news/us-news/department-energy-says-it-was-hacked-suspected-russian-campaign-n1251630. (accessed: 03 Jun. 2022).

14. Bannister, A. *Wind turbine giant Vestas confirms data breach following 'cybersecurity incident'*. Availible at: https://portswigger.net/daily-swig/wind-turbine-giant-vestas-confirms-data-breach-following-cybersecurity-incident (accessed: 03 Jun. 2022).

15. *Cyber Attacks on the Power Grid. Industroyer2*. Available at: https://securityboulevard.com/2022/05/cyber-attacks-on-the-power-grid/. (accessed: 04 Jun. 2022).

16. Akoto, P. *Enercon: Thousands of wind turbines need new hardware*. Access mode: https://www.energate-messenger.com/news/220914/enercon-thousands-of-wind-turbines-need-new-hardware. – 04 Jun. 2022.

17. *Deutsche Windtechnik hit by cyber attack*. Availible at: https://renews.biz/77220/deutsche-windtechnik-hit-by-cyber-attack/ (Accessed 03 Jun. 2022).

18. David, B. *Wind Turbine Giant Nordex Hit By Cyber-Attack*. Available at: https://www.infosecurity-magazine.com/news/wind-turbine-nordex-cyber-attack/#:~:text=German%20wind%20turbine%20manufacturer%2C%20Nordex%20Group%2C%20was%20hit,to%20Nordex%2C%20and%20response%20measures%20were%20taken%20quickly./ (accessed: 03 Jun. 2022).

19. *Threat landscape for industrial automation systems. Vulnerabilities identified in 2019.* Available at: https://ics-cert.kaspersky.com/publications/reports/2020/04/24/threat-landscape-for-industrial-automation-systems-vulnerabilities-identified-in-2019/. (accessed: 04 Jun. 2022).

20. Nikolopoulos, D., Moraitis, G., Bouziotas, D., Lykou, A., Karavokiros, G., Makropoulos, C. Cyber-Physical Stress-Testing Platform for Water Distribution Networks. *Journal of Environmental Engineering*, 2020, vol. 146, no. 7, 22 p. DOI: 10.1061/(ASCE)EE.1943-7870.0001722.

21. Kamchatnyy, M. Osnovni oznaky ponyattya "kiberviyna" u suchasnomu mizhnarodnomu pravi [The main features of the concept of "cyberwar" in contemporary international law]. *Al'manakh mizhnarodnoho prava – Almanac of international law*, 2017, no. 15, pp. 12-22.

22. *Chto takoye Khaktivizm? Kampanii, kotoryye sformirovali dvizheniye* [What is Hacktivism? Companies that formed the movement]. Available at: https://www.securitylab.ru/blog/company/PandaSecurityRus/348956.php. (accessed: 03 Jun. 2022).

23. *Kryminal'na vidpovidal'nist' za kiberzlochyny* [Criminal liability for cybercrime]. Available at: https://wiki.legalaid.gov.ua/index.php/Кримінальна_відповідальність_за_кіберзлочини. (Accessed: 03 Jun. 2022).

24. *What is the Morris worm? History and modern impact*. Available at: https://www.okta.com/uk/identity-101/morris-worm/ (accessed: 03 Jun 2022).

25. *Entsyklopediya zahroz ESET. Shcho take troyan?* [ESET Threat encyclopedy. What is a Trojan?]. Available at: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/troyan/. (accessed: 03 Jun. 2022).

26. *Injection attacks*. Available at: https://www.ibm.com/docs/en/snips/4.6.0?topic=categories-injection-attacks. (accessed: 04 Jun. 2022).

27. *What is a man-in-the-middle-attack?* Available at: https://www.ionos.com/digitalguide/server/security/man-in-the-middle-attack-an-overview-of-attack-patterns/. (accessed: 04 Jun. 2022).

28. Alotaibi, F., Lisitsa, A. Matrix profile for DDoS attacks detection. *Proceedings of the 16th Conference on Computer Science and Intelligence Systems, September 2–5, 2021. ACSIS*, 2021, vol. 25, pp. 357-361. DOI: 10.15439/2021F114.

29. *Fakhivtsi z kiberzakhystu rozpovily pro oznaky zlomu akauntiv v sotsmerezhakh* [Cyber defense experts spoke about the signs of hacking accounts in social networks]. Available at: https://www.unian.ua/science/10963961-fahivci-z-kiberzahistu-rozpovili-pro-oznaki-zlomu-akauntiv-v-socmerezhah.html. (accessed: 04 Jun. 2022).

30. Lee, K., Whiting, B. *Banking Systems, Types and Components*. Available at: https://study.com/academy/lesson/banking-system-definition-types.html. (accessed: 04 Jun. 2022).

31. Femi, J. G. Smart Water Management System. *International Journal of Smart Sensor and Adhoc Network*, 2022, vol. 3, no. 2, pp. 9-16. DOI: 10.47893/IJSSAN.2022.1213.

32. Kostrov, D. "Umnyye seti elektrosnabzheniya" (smart grid) i problemy s kiberbezopasnost'yu ["Smart grids" (smart grid) and problems with cybersecurity]. Available at: https://lib.itsec.ru/articles2/in-ch-sec/umnye-seti-elektrosnabzheniya-smart-grid-i-problemy-s-kiberbezopasnostyu. (Accessed: 04 Jun. 2022).

33. Al-Badi, A. H., Ahshan, R., Hosseinzadeh, N., Ghorbani, R., Hossain, E. Survey of Smart Grid Concepts and Technological Demonstrations Worldwide Emphasizing on the Oman Perspective. *Applied System Innovation*, 2020, vol. 3, no. 1. 27 p. DOI: 10.3390/asi3010005.

34. Goud, N. *Utah Wind and Solar Power Generation hit by a Cyber Attack*. Available at: https://www.cybersecurity-insiders.com/utah-wind-and-solar-power-generation-hit-by-a-cyber-attack/. (Accessed: 05 Jun. 2022).

35. Young, S. N., Peschel, J. M. Review of Human–Machine Interfaces for Small Unmanned Systems With Robotic Manipulators, *IEEE Transactions on Human-Machine Systems*, 2020, vol. 50, no. 2, pp. 131-143. DOI: 10.1109/THMS.2020.2969380.

36. Abrahamsen, F. E., Ai, Y., Cheffena, M. Communication Technologies for Smart Grid: A Comprehensive Survey. *Sensors*, 2021, vol. 21, no. 23, article no. 8087. 24 p. DOI: 10.3390/s21238087.

37. *etap iCE™ - Intelligent Control Enterprise Hardware*. Available at: https://etap.com/product/etapiCE-DAC-Hardware. (Accessed: 05 Jun. 2022).

38. Tan, S., Guerrero, J., Xie, P. et al. Brief Survey on Attack Detection Method for Cyber-Physical Systems. *IEEE Systems Journal*, 2020, vol. 14, no. 4, pp. 5329-5339. DOI: 10.1109/JSYST.2020.2991258.

39. *Roadmap for Wind Cybersecurity. U.S. Department of Energy (DOE) Energy Efficiency and Renewable Energy (EERE).* Wind Energy Technologies Office, 2020. 84 p.

40. Yohanandhan, R. V., Elavarasan, R., Manoharan, O., Mihet-Popa, I. Cyber-Physical Power System (CPPS): A Review on Modeling, Simulation, and Analysis With Cyber Security Applications. *IEEE Access*, 2020, vol. 8, pp. 151019-151064. DOI: 10.1109/ACCESS.2020.3016826.

41. Ponochovniy, Y. L., Kharchenko, V. S. Metodolohiya zabezpechennya harantozdatnosti informatsiyno-keruyuchykh system z vykorystannyam bahatotsil'ovykh stratehiy obsluhovuvannya [Dependability assurance methodology of information and control systems using multipurpose service strategies]. *Radioelektronni i komp'uterni sistemi - Radioelectronic and computer systems*, 2020, no. 3(95), pp. 43-58. DOI: 10.32620/reks.2020.3.05.

42. Odarushchenko, O. M., Odarushchenko, O. B., Kharchenko, V. S. Markovs'ki modeli otsinyuvannya funktsional'noyi bezpeky prohramno-tekhnichnykh kompleksiv na samodiahnostovnykh prohramovnykh platformakh z urakhuvannyam pomylok zasobiv kontrolyu [Markov models for functional safety assessment of instrumentation and control systems based on self-checking programmable platforms]. *Radioelektronni i komp'uterni sistemi - Radioelectronic and computer systems*, 2019, no. 4(92), pp. 17-29. DOI: 10.32620/reks.2019.4.02

43. Mohammadpourfard, M., Genc, I., Lakshminarayana, S., Konstantinou, C., Attack Detection and Localization in Smart Grid with Image-based Deep Learning. *2021 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, 2021, pp. 121-126. DOI: 10.1109/SmartGridComm51999.2021.9631994.

44. Rashed, M., Gondal, I., Kamruzzaman, J., Islam, S. State Estimation within IED Based Smart Grid Using Kalman Estimates. *Electronics*, 2021, vol. 10, no. 15, article no. 1783. 6 p. DOI: 10.3390/electronics10151783.

45. Fursov, I. I., Shmatko, O. V. Analiz statystychnykh pokaznykiv dyspersiyi, asymetriyi ta ekstsesu pry vyznachenni porushen' informatsiynoyi bezpeky kiberfizychnykh system vitrovykh heneratoriv [Analysis of

statistical indicators of variance, asymmetry and excess in determining information security violations of cyber-physical systems of wind turbines]. *Radioelektronni i komp'uterni sistemi – Radioelectronic and computer systems*, 2021, no. 4, pp. 132-144. DOI: 10.32620/reks.2021.4.11.

46. Lysenko, S. M., Kharchenko, V. S., Bobrovnikova, K. Y., Shchuka, R. V. Computer systems resilience in the presence of cyber threats: taxonomy and ontology [Rezyl'yentnist' kom''yuternukh system v umovakh kiberzahroz: taksonomiya ta ontolohiya]. *Radioelektronni i komp'uterni sistemi - Radioelectronic and computer systems*, 2020, no. 1(93), pp. 17-28. DOI: 10.32620/reks.2020.1.02.

47. Rehmani, M. H., Davy, A., Jennings, B., Assi, C. Software-Defined Networks-Based Smart Grid Communication: A ComprehensiveSurvey. *IEEE Communications Surveys & Tutorials*, 2019, vol. 21, iss. 3, pp. 2637-2670. DOI: 10.1109/COMST.2019.2908266.

48. Raza, N., Akbar, Q. M, Soofi, A., Akbar, S. Study of Smart Grid communication network architectures and technologies. *Journal of Computer and Communications*, 2019, vol. 7, no. 3, pp. 19-29. DOI: 10.4236/jcc.2019.73003.

Надійшла до редакції 05.09.2022, розглянута на редколегії 20.11.2022

SMART GRID ТА ВІТРОВІ ГЕНЕРАТОРИ: ОГЛЯД КІБЕРЗАГРОЗ ТА ВРАЗЛИВОСТЕЙ МЕРЕЖ ЕЛЕКТРОПОСТАЧАННЯ

Ігор Фурсов, Клим Ямковий, Олександр Шматко

Предметом даного дослідження є кіберуразливість вітрогенераторів, як частини кіберфізичних систем інтелектуальних мереж електропостачання, Smart Grid. Вітрогенератори виробляють електроенергію для подальшого розподілу в мережі між «розумними» споживачами електроенергії, до яких часто відносяться автономні системи живлення у медичних установах, автономне електропостачання будинків, зарядні станції для автомобілів і т.д. Вітрогенератори працюють у двох площинах: у фізичному та інформаційному просторі. Таким чином, порушення безпеки інформаційного потоку вітрогенератора може вплинути на фізичні показники вироблення електроенергії, вивести з ладу обладнання. **Метою** дослідження є виявлення типів кіберзагроз в мережі вітрогенераторів на основі аналізу відомих інцидентів атак, аналізу структури мережі Smart Grid, мережевих пристроїв, протоколів і механізмів управління вітрогенератором. **Завданнями** роботи є: огляд та аналіз відомих інцидентів кібератак; огляд класифікації кіберзагроз; огляд найбільш поширених методів атак на кіберфізичні системи вітрових генераторів; огляд способів вторгнень в інформаційний потік кіберфізичних систем вітрогенератора; огляд механізмів відмовостійкості вітрових генераторів у випадку кібератаки; огляд напрямків подальших досліджень. **Методами** досліджень є системний підхід, який забезпечує всебічне вивчення проблеми, кількісний та якісний аналіз інцидентів кібератак на вітрогенератори і методів атак. Були отримані наступні **результати**: проаналізовані 11 відомих маштабних кібератак на кіберфізичні системи енергетичного сектора та інтелектуальні мережі електропостачання, вітрові генератори, розглянуті характеристики інформаційних потоків і структура вітрових генераторів. Були розглянуті основні комунікаційні інтерфейси мережі Smart Grid, розглянуті механізми управління фізичними частинами системи вітрового генератора, такі як автоматичний регулятор напруги, система управління генерацією електроенергії, проаналізовані вразливі протоколи передачі даних, зокрема DNP3, розглянуті наслідки у разі кібервторгнення в мережі. **Висновки**: вітряні електростанції, як частина системи Smart Grid, є зручною мішенню для кібератак, оскільки кількість потенційних способів втручання в інформаційний потік кіберфізичних систем зростає через зростання сенсорних мереж, каналів зв'язку у мережі. Це особливо важливо для подальшого розвитку систем безпеки вітроелектростанцій, які в даний час не здатні забезпечити високу точність виявлення вторгнень в інформаційний потік.

Ключові слова: кіберзагроза; Smart Grid; КФС; кібербезпека; вітрові генератори.

Фурсов Ігор Ігорович – асп. каф. програмної інженерії та інформаційних технологій управління, Національний технічний університет «Харківський політехнічний інститут», Харків, Україна.

Ямковий Клим Сергійович – асп. каф. комп’ютерної математики і аналізу даних, Національний технічний університет «Харківський політехнічний інститут», Харків, Україна.

Шматко Олександр Віталійович – канд. техн. наук, доц. каф. програмної інженерії та інформаційних технологій управління, Національний технічний університет «Харківський політехнічний інститут», Харків, Україна.

Ihor Fursov – PhD student of the SEMIT Department, National Technical University «Kharkiv Polytechnic Institute», Kharkiv, Ukraine, e-mail: ihor.fursov@gmail.com, ORCID: 0000-0002-3597-4935.

Klym Yamkovyi – PhD student of the CMDA Department, National Technical University «Kharkiv Polytechnic Institute», Kharkiv, Ukraine, e-mail: yamkovou@gmail.com, ORCID: 0000-0001-9512-4150.

Oleksandr Shmatko – Candidate of Technical Sciences, Associate Professor of the SEMIT Department, National Technical University «Kharkiv Polytechnic Institute», Kharkiv, Ukraine, e-mail: asu.spios@gmail.com, ORCID: 0000-0002-2426-900X.